Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bundesdatenschutzgesetz
- Text und Erläuterung -

Info 1

BfDI – Info 1

Bundesdatenschutzgesetz
- Text und Erläuterung -

Impressum

Herausgeber:
Der Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit

Postfach 20 01 12, 53131 Bonn
Hausanschrift: Husarenstraße 30, 53117 Bonn
Tel. +49 (0) 228 997799-0
Fax +49 (0) 228 997799-550
E-Mail: poststelle@bfdi.bund.de
Internet: www.datenschutz.bund.de

Druck: Druckpartner Moser
Druck + Verlag GmbH
Römerkanal 52-54
53359 Rheinbach

Auflage: 15. Auflage, Januar 2011

Inhaltsverzeichnis

Vorwort 5

1 Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit 7

2 Sicherung des Persönlichkeitsrechts durch das Bundesdatenschutzgesetz 11
2.1 Ziel des Datenschutzes 11
2.2 Einführung in das Datenschutzrecht 13
2.3 Anwendungsbereich des Bundesdatenschutzgesetzes 15
2.4 Grundsätzlich ist verboten, was nicht ausdrücklich erlaubt ist! 19
2.5 Zweckbindungsgrundsatz 20
2.6 Datenerhebung 24
2.7 Übermittlung von Daten 26
2.8 Vorherige Kontrolle risikoreicher Datenverarbeitung (sog. Vorabkontrolle) 28
2.9 Technische und organisatorische Sicherung des Datenschutzes 30
2.10 Der behördliche und betriebliche Beauftragte für den Datenschutz 32
2.11 Datenverarbeitung im Auftrag 35
2.12 Die wichtigsten Änderungen im Überblick 36

3 Besonderheiten bei der Datenverarbeitung durch nicht-öffentliche Stellen, Privatwirtschaft, Vereine etc. 38
3.1 Rechtsgrundlagen der Datenverarbeitung 38
3.2 Werbung und Adresshandel 39
3.3 Die Tätigkeit von Auskunfteien 41
3.4 Scoring 42

4 Rechte der Bürgerinnen und Bürger 44
4.1 Das Recht auf Auskunft 44
4.2 Das Einsichtsrecht in das Verfahrensverzeichnis 48
4.3 Die Rechte auf Benachrichtigung, Berichtigung, Sperrung oder Löschung 50
4.4 Das allgemeine Widerspruchsrecht 53
4.5 Die Rechte bei automatisierten Einzelentscheidungen 54
4.6 Die Rechte beim Einsatz von Videoüberwachung 55
4.7 Das Recht auf Anrufung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sowie anderer Kontrollinstitutionen 57

4.8 Das Recht auf Schadensersatz 58

5 Seien Sie Ihr eigener Datenschutzbeauftragter! 59

6 Begriffe und ihre Bedeutung 60

Anhang 1: *Bundesdatenschutzgesetz (Gesetzestext)* 63

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*..... 116

Anhang 3: *Auszug aus dem Urteil des Ersten Senats des Bundesverfassungsgerichts vom 15. Dezember 1983 – 1BvR 209/83 u. a. – sog. Volkszählungsurteil* 157

Anhang 4: *Auszug aus dem Urteil des Ersten Senats des Bundesverfassungsgerichts vom 27. Februar 2008 – 1 BvR 370/07, 1 BvR 595/07 -* 162

Anhang 5: *Anschriften der Datenschutzbeauftragten des Bundes und der Länder* 176

Anhang 6: *Anschriften der Aufsichtsbehörden für den nichtöffentlichen Bereich* 178

Anhang 7: *Anschriften der Rundfunkbeauftragten für den Datenschutz* 180

Anhang 8: *Informationen zum Datenschutz im Internet*..... 182

Anhang 9: *Organigramm des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit* 183

Vorwort

Das Bundesdatenschutzgesetz soll dazu beitragen, das Grundrecht auf informationelle Selbstbestimmung zu verwirklichen. Es setzt die Europäische Datenschutzrichtlinie 95/46/EG vom 24. Oktober 1995 um, die für den ganzen Europäischen Wirtschaftsraum einheitliche Datenschutzstandards gesetzt hat.

Die massenhafte, vom Betroffenen häufig unbemerkte Datenerhebung und -verarbeitung ist eine beunruhigende Nebenwirkung der Informationsgesellschaft. Nie zuvor in der Geschichte wurde unser Verhalten, das ganze Leben eines Menschen technisch so perfekt und vollständig abgebildet. Nicht nur Computer oder Handys sind mit digitalen Komponenten ausgerüstet, sondern auch viele Gegenstände unseres Alltags. Nahezu jede Verwendung technischer Geräte hinterlässt eine Datenspur, die dem jeweiligen Nutzer in den meisten Fällen direkt zugeordnet werden kann.

Welche Aufgabe kann dem Datenschutz hier zukommen?

Datenschutz ist kein Selbstzweck. Vielmehr steht die Sicherung und Verwirklichung eines Grundrechts im Mittelpunkt, das unmittelbar aus der Menschenwürde und der freien Entfaltung der Persönlichkeit folgt. Der Datenschutz kann den Einzelnen nicht vor jeglicher Form von Verarbeitung seiner Daten bewahren, aber er soll es ihm ermöglichen, grundsätzlich selbst darüber zu bestimmen, „wer was über ihn weiß“.

Die zunehmende Komplexität technologischer Systeme geht jedoch vielfach mit einem Verlust an Transparenz einher. Umso wichtiger ist eine Komplexitätsreduktion, bei der die wesentlichen Informationen vermittelt und dem Einzelnen die Möglichkeit zur Entscheidung über echte Alternativen gegeben wird.

Diese Informationsbroschüre will dazu beitragen, das Datenschutzrecht verständlich darzustellen, die Bürgerinnen und Bürger über ihre Rechte zu informieren und ihnen zu helfen, zum Schutz ihrer eigenen Daten aktiv zu werden. Sie enthält neben dem Gesetzestext und weiteren wich-

tigen Materialien eine kurze Einführung in die nicht immer einfache Materie. Zugleich eignet sie sich als Basisinformation auch für diejenigen, die beruflich mit personenbezogenen Daten umgehen.

Bonn, im Januar 2011

Peter Schaar

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

1. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Gesetzesbestimmungen: §§ 22 bis 26 Bundesdatenschutzgesetz (BDSG)

Die Institution des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit besteht seit 1978. Seit dem 17. Dezember 2003 ist Peter Schaar Bundesbeauftragter für den Datenschutz. Seit dem 1. Januar 2006 ist ihm auch die Aufgabe des Bundesbeauftragten für die Informationsfreiheit übertragen. Er wurde vom Deutschen Bundestag am 26. November 2008 für weitere fünf Jahre in seinem Amt bestätigt.

Dem Bundesbeauftragten stehen bei der Wahrnehmung seiner Aufgaben derzeit etwa 80 Mitarbeiterinnen und Mitarbeiter in Bonn und in Berlin zur Seite. Die Organisation und Aufgabenverteilung sind im Anhang 9 dargestellt.

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

Hauptaufgaben des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit 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 Bundesministerien (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 11.000 schriftlichen und mündlichen Eingaben und Anfragen im Jahr kontrollierend und auch beratend als Anwalt der Bürgerinnen und Bürger tätig (vgl. Kapitel 4.8).

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, der Bundespolizei, der Bundeswehr, die Wasser- und Schifffahrtsdirektionen wie auch bestimmte Träger der sozialen Sicherung, z.B. die Agenturen für Arbeit, gesetzliche Krankenkassen, Unfallkassen oder die Deutsche Rentenversicherung Bund. 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 nicht zu großzügig verfahren wird. Die Kontrollergebnisse werden in einem schriftlichen Kontrollbericht niedergelegt.

Tätigkeitsberichte

Wer mehr über die Tätigkeit des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wissen möchte, kann dies in seinen Tätigkeitsberichten nachlesen. Der Tätigkeitsbericht, in dem der Bundesbeauftragte den Bundestag und die Öffentlichkeit alle zwei Jahre über die wesentlichen Entwicklungen im Datenschutz und die Schwerpunkte seiner Aufgabenwahrnehmung unterrichtet, kann – wie auch andere Informationsmaterialien – kostenlos unter folgender Anschrift angefordert werden:

Der Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit
Husarenstraße 30
53117 Bonn
E-Mail: poststelle@bfdi.bund.de

Die Tätigkeitsberichte und viele weitere Informationsmaterialien stehen auch in elektronischer Form unter folgender Internet-Adresse zum Abruf bereit:

www.datenschutz.bund.de

Der Bundesbeauftragte kann Kritik und Vorschläge gegenüber den Ministerien und sonstigen Bundesbehörden, dem Parlament und der Öffentlichkeit äußern. Weisungsrechte besitzt er nicht. Der Bundesbeauftragte hat auch die Möglichkeit, einen festgestellten Datenschutzverstoß bei den Strafverfolgungsbehörden anzuzeigen und Strafantrag zu stellen.

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 Unterstützung von Vorschlägen des Bundesbeauftragten oder durch Formulierung entsprechender Prüfungsbitten an die Bundesregierung,

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

– durch Anregungen, die Verwaltungspraxis datenschutzfreundlicher zu gestalten oder über bestimmte Problembereiche gesondert Bericht zu erstatten.

Die Rechtsstellung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

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

Der Bundesbeauftragte ist in der Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. Weder einzelne Minister noch die Bundesregierung können ihm fachaufsichtliche Weisungen in Bezug auf seine Amtstätigkeit geben. Er untersteht allerdings der Rechtsaufsicht der Bundesregierung und nur hinsichtlich dienstrechtlicher Fragen der Dienstaufsicht des Bundesministeriums des Innern.

Nachdem der Europäische Gerichtshof in einem Urteil vom 9. März 2010 (Az.: C-518/07) festgestellt hat, dass die Bundesrepublik Deutschland gegen die Verpflichtung aus Artikel 28 der Europäischen Datenschutzrichtlinie (Richtlinie 95/46/EG) verstößt, weil die Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich nicht völlig unabhängig sind, stellt sich auch die Frage, ob die derzeitigen Vorschriften zur Rechts- und

Dienstaufsicht über den Bundesbeauftragten mit den europarechtlichen Vorgaben vereinbar sind.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit 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 hat auch Zugang zu Unterlagen, die einer besonderen Geheimhaltung unterliegen (vgl. dazu § 24 Absatz 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. Bürgerinnen und Bürger können sich ihm 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.

2 Sicherung des Persönlichkeitsrechts durch das Bundesdatenschutzgesetz

2.1 Ziel des Datenschutzes

Gesetzesbestimmungen: § 1 Absatz 1 Bundesdatenschutzgesetz (BDSG), Artikel 1 und 2 Grundgesetz

Der Datenschutz soll den Menschen vor der Gefährdung durch die nachteiligen Folgen einer Datenverarbeitung schützen. § 1 Absatz 1 BDSG umschreibt dies so:

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

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 Absatz 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 Absatz 1 Grundgesetz)

Diese Verfassungsartikel sind auch die Grundlage des Datenschutzes. Das Bundesverfassungsgericht hat dazu im sog. Volkszählungsurteil vom 15. Dezember 1983 (Auszug als Anhang 3 abgedruckt) Folgendes festgestellt:

„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 Bundesverfassungsgericht hat auch nach dem Volkszählungsurteil immer wieder den Schutz der Privatsphäre gestärkt. Im Februar 2008 hat das Gericht seine Rechtsprechung zum Schutz des Persönlichkeitsrechts angesichts fortschreitender technischer Möglichkeiten durch Formulierung eines „Grundrechts aufs Gewährleistung der Vertraulichkeit und Integrität der informationstechnischen Systeme" weiterentwickelt (1 BvR 370/07; 1 BvR 595/07; Auszug als Anhang 4 abgedruckt). Ebenso wie das Recht auf informationelle Selbstbestimmung ist es eine besondere Ausprägung des allgemeinen Persönlichkeitsrechts, geht aber über das Individual-Grundrecht auf informationelle Selbstbestimmung hinaus. Es schützt die Bürgerinnen und Bürger vor den neuartigen Gefahren, die mit der Nutzung von vernetzten Computern, mobilen und multifunktionalen Geräten verbunden sind. Das Grundrecht schützt das Vertrauen der Berechtigten, selbst über ihr System, dessen Leistungen, Funktionen und Inhalte bestimmen zu können.

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 Artikel 8 der Charta der Grundrechte der Europäischen Union aufgenommen. 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 (als Anhang 2 abgedruckt) gibt in Artikel 1 Absatz 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. Seit Inkrafttreten des Vertrags von Lissabon ist die Charta der Grundrechte nicht nur für die Europäische Union und ihre Institutionen, sondern auch für die Mitgliedstaaten bindendes Recht.

Wesentliche Bestimmungen des Bundesdatenschutzgesetzes werden im Folgenden vorgestellt.

2.2 Einführung in das Datenschutzrecht

Das Bundesdatenschutzgesetz (BDSG) stellt Regeln für den Umgang mit personenbezogenen Daten auf. Jegliche Verarbeitung von personenbezogenen Daten bedarf einer ausdrücklichen Erlaubnis, sei es durch ein Gesetz oder durch eine Einwilligung des Einzelnen. Das Gesetz enthält Schutzregelungen für das informationelle Selbstbestimmungsrecht. Dazu gehören 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 und die Bürger über den Umgang mit ihren Daten zu informieren. Es weist aber auch den betroffenen Bürgerinnen und Bürgern eine Reihe von Rechten ausdrücklich zu.

Vorrangiges Ziel des Datenschutzes ist es, eine Gefährdung des Persönlichkeitsrechts des Einzelnen von vorneherein zu verhindern durch das Aufstellen von Verwendungsregeln für personenbezogene Daten und über die Gestaltung und den Einsatz von Informationstechnik.

Die Entwicklung und der Einsatz datenschutzfreundlicher IT-Systeme hat zunehmende Bedeutung. Im Mittelpunkt steht dabei, dass möglichst keine personenbezogenen Daten, oder – wo das nicht möglich ist – so wenig wie möglich personenbezogene Daten verwendet werden. Riesige Datenmengen sollen erst gar nicht entstehen (Datenvermeidung bzw. Datensparsamkeit). Die technisch-organisatorischen Maßnahmen, die nach § 9 und seiner dazu ergangenen Anlage zu treffen sind, sollen die Daten u. a. gegen unerlaubten Zugriff und Verwendung sichern.

Die Datenschutzaufsicht ist mehr als eine begleitende und ggf. sanktionierende Kontrollinstanz. Einen Schwerpunkt ihrer Arbeit bildet die vorbeugende Beratung. Behörden und Unternehmen, Bürgerinnen und Bürger sollten daher keine Scheu haben, bei den Datenschutzbehörden Rat zu suchen.

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

Dabei können sie die Hilfe der Datenschutzbehörden in Anspruch nehmen. Auch die Verantwortung der Daten verarbeitenden 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 in Behörde und Betrieb inne. Sie sind Triebkraft des Datenschutzes in ihrer Behörde oder in ihrem Betrieb und zugleich Koordinatoren für alle Datenschutzmaßnahmen. Gleichzeitig sind sie Ansprechpartner für Bürgerinnen und Bürger.

Wenn es zu einem Verstoß gegen Datenschutzrecht und einem Schaden gekommen ist, bleibt dies nicht ohne Folgen. Der Gesetzgeber hat kürzlich die bestehenden Bußgeldvorschriften im BDSG erweitert und die Bußgeldhöhe angehoben. Die Rechtsstellung der Aufsichtsbehörden

wurde erheblich gestärkt. Diese haben erstmals wirksame Handlungsmöglichkeiten und können strittige Auslegungsfragen gerichtlich klären lassen. Zudem wurde eine neue Pflicht zur Information der Betroffenen und der Datenschutzaufsichtsbehörden bei Datenschutzpannen geschaffen.

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

2.3 Anwendungsbereich des Bundesdatenschutzgesetzes

Gesetzesbestimmungen: §§ 1 Absatz 2 und 3, 2, 12, 27 BDSG

Das Bundesdatenschutzgesetz gilt uneingeschränkt für öffentliche Stellen des Bundes und für nicht-öffentliche Stellen (Private). Nur sehr eingeschränkt gilt es für die Rundfunkanstalt des Bundes, die Deutsche Welle. Es findet keine Anwendung bei den öffentlichen Stellen der Länder und im Bereich der Kirchen. Weitgehende Ausnahmen gibt es auch für Presseunternehmen, soweit sie personenbezogene Daten ausschließlich zu journalistisch-redaktionellen Zwecken verarbeiten. Bereichsspezifische Regelungen gehen dem Bundesdatenschutzgesetz vor.

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.

Die Länder haben jeweils Landesdatenschutzgesetze, welche den Umgang der Landesbehörden mit personenbezogenen Daten regeln. Nähere Informationen erhalten Sie bei den Landesbeauftragten für den Datenschutz (Anschriften siehe Anhang 5).

Beispiele:
***Behörden** des Bundes sind die Ministerien und alle ihnen nachgeordneten Behörden, etwa die Bundespolizeidirektionen, die Bundesfinanzdirektionen oder die Wasser- und Schifffahrtsdirektionen.*
***Organe der Rechtspflege** sind die Bundesgerichte (z. B. Bundesgerichtshof, Bundesverwaltungsgericht) sowie der Generalbundesanwalt.*
***Andere öffentlich-rechtliche Einrichtungen** sind die Agenturen für Arbeit, die Deutsche Rentenversicherung Bund oder die Stiftung Preußischer Kulturbesitz.*
Vereinigungen öffentlicher Stellen *sind die Gesellschaft für Technische Zusammenarbeit (GTZ) oder die Kunst- und Ausstellungshalle der Bundesrepublik Deutschland GmbH.*

***Öffentliche Stellen der Länder** sind etwa Landesministerien, Polizeibehörden, Kommunen, Universitäten, öffentlich-rechtliche Rundfunkanstalten (außer der Deutschen Welle, die eine Bundesrundfunkanstalt ist), Schulen, staatliche und kommunale Krankenhäuser.*

Nicht-öffentliche Stellen sind

- juristische Personen und Personenvereinigungen des Privatrechts.
- Auch natürliche Personen können nicht-öffentliche Stellen im Sinne des Datenschutzrechts sein, soweit sie personenbezogene Daten verarbeiten.

Soweit Private hoheitliche Aufgaben der öffentlichen Verwaltung wahrnehmen (etwa als „beliehene Unternehmer“ tätig werden), sind sie allerdings öffentliche Stellen.

Beispiel:
Nach § 9a Absatz 1 des Handelsgesetzbuches und der eBundesanzeiger-Verordnung führt die Bundesanzeiger Verlagsgesellschaft mbH als Beliehene das Unternehmensregister. Sie ist hinsichtlich der Verarbeitung personenbezogener Daten im Zusammenhang mit der Erfüllung dieser Aufgabe als öffentliche Stelle anzusehen. Hinsichtlich ihrer sonstigen Geschäftstätigkeit ist das Unternehmen hingegen eine nicht-öffentliche Stelle.

Nicht-öffentliche Stellen unterliegen dem Bundesdatenschutzgesetz 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.

Beispiel:
Das Führen eines privaten Adressbuchs – auch in elektronischer Form – oder das Sammeln personenbezogener Daten zur Pflege eines Hobbys fallen nicht unter das Datenschutzrecht. Auch die Videoüberwachung des Nachbargrundstücks zu rein privaten Zwecken fällt nicht unter das Datenschutzrecht, kann aber zu berechtigten zivilrechtlichen Unterlassungs- und Beseitigungsansprüchen führen. Die Videoüberwachung eines öffentlich zugänglichen Raumes durch eine Privatperson zum Zwecke der Gefahrenabwehr oder Beweissicherung ist hingegen keine private Tätigkeit mehr.

Das Bundesdatenschutzgesetz 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 Bundesdatenschutzgesetz im öffentlichen Bereich auch für Daten in Akten und anderen Unterlagen gilt. Über die bereits genannten Einschränkungen im nicht-öffentlichen Bereich hinaus gilt das Bundesdatenschutzgesetz dort auch für solche personenbezogenen Daten, die offensichtlich aus einer automatisierten Verarbeitung entnommen worden sind, etwa für listenmäßige Ausdrucke aus Dateien.

Kirchen, Religionsgemeinschaften und kirchliche Einrichtungen

Mit Blick auf die verfassungsrechtlich garantierte Autonomie von öffentlich-rechtlichen Religionsgemeinschaften gilt das Bundesdatenschutzgesetz in diesem Bereich (einschließlich der angeschlossenen kirchlichen karitativen Einrichtungen) nicht. Die Evangelischen Kirchen in Deutschland und die Bistümer der Katholischen Kirche in Deutschland und andere Religionsgemeinschaften haben eigene Datenschutzvorschriften erlassen. Diese sind jedoch weitestgehend an die Bestimmungen des Bundesdatenschutzgesetzes angepasst und sehen auch die Einrichtung kirchlicher Datenschutzbeauftragter vor (siehe dazu Kapitel 4.7).

Rundfunkanstalten

Aufgrund der verfassungsrechtlich garantierten Rundfunkfreiheit gelten auch für die journalistisch-redaktionelle Arbeit in den öffentlich-rechtlichen und privaten Rundfunkanstalten (Fernsehen und Hörfunk) die allgemeinen datenschutzrechtlichen Bestimmungen nur eingeschränkt. An ihre Stelle treten rundfunkspezifische Datenschutzvorschriften, die einen Ausgleich zwischen dem Grundrecht auf informationelle Selbstbestimmung und dem Grundrecht der Rundfunkfreiheit zu erreichen suchen. Von Bedeutung ist hierfür der Rundfunkstaatsvertrag, der nach seinem § 1 in gleicher Weise die Grundlage für den öffentlich-rechtlichen, wie den privaten Rundfunk bildet und in § 47 den Datenschutz regelt.

Besonderheiten bestehen auch bei der Datenschutzkontrolle. Weitere Ausführungen dazu finden sich in Kapitel 4.7.

Bereichsspezifische Regelungen

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, etwa

– das Sozialgesetzbuch,

– das Bundesverfassungsschutzgesetz,

– das Bundespolizeigesetz,

– das Telekommunikationsgesetz.

Diese – und viele weitere – sog. „bereichsspezifischen Regelungen“ gehen dem Bundesdatenschutzgesetz vor.

Beispiele:

- *Eine gesetzliche Krankenkasse kann Sozialdaten nur nach den §§ 67d ff. SGB X sowie speziellen Vorschriften des SGB V übermitteln. Ein Rückgriff auf das BDSG ist ausgeschlossen.*
- *Die Bundespolizei kann sich bei der Erhebung personenbezogener Daten nur auf die §§ 21 ff. BPolG stützen. § 13 BDSG ist nicht anwendbar.*
- *Ein Telekommunikationsanbieter darf seine Bestandsdaten nur im Rahmen von § 95 TKG zu Werbezwecken nutzen. Es ist ihm nicht erlaubt, auf die – weniger strikten – allgemeinen Vorschriften in § 28 BDSG zurückzugreifen.*

2.4 Grundsätzlich ist verboten, was nicht ausdrücklich erlaubt ist!

Gesetzesbestimmungen: §§ 4, 4a, 28 BDSG

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

– sie sind durch eine Rechtsvorschrift ausdrücklich erlaubt oder angeordnet oder

– 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 muss tatsächlich freiwillig sein.
- Die Einwilligung bedarf grundsätzlich der Schriftform. Davon darf nur abgewichen werden, wenn wegen besonderer Umstände eine andere Form angemessen ist.

- Der Betroffene ist vorher über die Tragweite seiner Einwilligung aufzuklären (insbesondere über den Verarbeitungszweck und die verantwortliche Stelle).

- Er ist auch darüber zu informieren, was geschieht, wenn er nicht einwilligt (z.B. dass Ansprüche verloren gehen können), soweit nach den Umständen des Einzelfalls erforderlich oder wenn er dies verlangt.

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

Besonders geregelt hat der Gesetzgeber die Einwilligung zu Werbezwecken (vgl. § 28). Näheres hierzu finden Sie im Kapitel 3.2 „Werbung und Adresshandel".

Bei der Verarbeitung besonderer Arten personenbezogener Daten gem. § 3 Absatz 9 (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 Zweckbindungsgrundsatz

Gesetzesbestimmungen: §§ 14, 28, 29, 31 BDSG

Personenbezogene Daten dürfen durch öffentliche Stellen gespeichert, verändert oder genutzt werden, soweit

– 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 voran ging: für die sie erstmalig gespeichert worden sind). Das heißt, dass personenbezogene Daten grundsätzlich nur zu den Zwecken verarbeitet werden dürfen, für die sie erhoben bzw. gespeichert worden sind (Zweckbindungsgrundsatz).

Beispiel:
Eine Behörde erhält von einem Bürger Namen und Anschrift, um ihm eine bestellte Broschüre liefern zu können. Die Übermittlung dieser Daten an den Spediteur wäre erforderlich, weil er anderenfalls nicht liefern könnte. Sie entspräche auch exakt der ursprünglichen Zweckbestimmung „Lieferung der Ware". Verkauft die Behörde die Daten hingegen an einen Adresshändler zum Zwecke der Werbung, entspricht dies nicht mehr der Zweckbestimmung – es bedarf dann einer Befugnis zur Zweckänderung.

Von diesem Grundsatz sieht das Gesetz aber eine Reihe Ausnahmen vor.

Welche Ausnahmen von der Zweckbindung gibt es?

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,

– zur Wahrung erheblicher Belange des Gemeinwohls,

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

„Besondere Arten personenbezogener Daten" sind in § 3 Absatz 9 BDSG definiert und beinhalten Angaben über

- rassische und ethnische Herkunft,
- politische Meinungen,
- religiöse oder politische Überzeugungen,
- Gewerkschaftszugehörigkeit,
- Gesundheit oder
- Sexualleben.

Das Gesetz schränkt die Möglichkeiten der Erhebung, Verarbeitung und Nutzung dieser Daten an vielen Stellen ein. Je nach Verwendungszusammenhang können aber auch andere Kategorien personenbezogener Daten ähnlich schutzwürdig sein.

Auf der anderen Seite stellt das Gesetz klar, dass eine Zweckänderung nicht vorliegt, soweit die Daten verwendet werden für

- 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 dagegen für Daten, die ausschließlich gespeichert werden zur Datenschutzkontrolle, Datensicherung, zur Sicherung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage oder zur wissenschaftlichen Forschung (§ 40).

Für die nicht-öffentlichen Stellen gilt der Zweckbindungsgrundsatz nur eingeschränkt. Bereits bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen (vgl. § 28 Absatz 1 Satz 2). Dies gilt auch für die geschäftsmäßige Datenverarbeitung (vgl. § 29 Absatz 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 oder eines Dritten,

– wenn die Daten allgemein zugänglich sind oder veröffentlicht werden dürften,

– zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten,

– zu wissenschaftlichen Zwecken.

Es muss stets zwischen den entgegenstehenden schutzwürdigen Interessen des Betroffenen und dem Interesse an der Zweckänderung abgewogen werden.

Beispiel:
Ein Inkassounternehmen möchte von einem Arbeitgeber Anschrift und Kontoverbindung eines Arbeitnehmers bekommen, um eine Forderung eintreiben zu können. Der Arbeitnehmer ist in einem sensiblen Bereich des Unternehmens tätig. Das Inkassounternehmen hat zwar ein berechtigtes Interesse, die schutzwürdigen Interessen des Arbeitnehmers überwiegen jedoch.

Für Zwecke des Adresshandels oder der Werbung dürfen personenbezogene Daten dagegen grundsätzlich nur mit Einwilligung des Betroffenen verarbeitet oder genutzt werden. Zu diesem grundsätzlichen Verbot gibt es jedoch eine Reihe von Ausnahmen. Näheres hierzu finden Sie im Kapitel 3.2. „Werbung und Adresshandel“.

2.6 Datenerhebung

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

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

Die Datenerhebung darf nur in dem erforderlichen Umfang erfolgen. Bei den öffentlichen Stellen heißt dies, dass die Daten für die Erfüllung der gesetzlichen Aufgaben erforderlich sind. Im nicht-öffentlichen Bereich wird der größte Teil der personenbezogenen Daten zur 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 rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnis (typischerweise Vertrag) mit dem Betroffenen ist Maßstab für die Datenerhebung der jeweils vereinbarte Zweck.

  Beispiel:
  Ein Vertrag zwischen Bank und Bankkunden, Arzt und Patienten, Versicherung und Versicherten; entsprechend eingeschränkt auch schon vor Vertragsabschluss und nach dessen Ende

- 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 Probleme wirft in diesem Zusammenhang der Umgang mit Informationen im Internet auf, die lediglich in einem regionalen oder sachlichen Kontext öffentlich zugänglich sind (zum Beispiel die systematische Erfassung von Straßenansichten). In diesen Fällen sind Widersprüche der Betroffenen zu beachten.

- 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 Absatz 2 Nr. 1–9, 28 Absatz 6 Nr. 1–4, sowie Absatz 7–9, 29 Absatz 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.

- 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. 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:

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),

– 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 oder

– 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 seine Datenschutzrechte wahrnehmen kann.

2.7 Übermittlung von Daten

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

Für öffentliche Stellen unterscheidet das Gesetz zwischen der Übermittlung an eine andere öffentliche Stelle oder eine nicht-öffentliche Stelle. 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).

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.

Beispiel:
Eine Behörde verfügt über Informationen, die die Beschädigung eines Grundstücks durch einen Dritten betrifft. Der geschädigte Eigentümer möchte nun von der Behörde Namen und Anschrift des Dritten wissen, um einen Schadensersatzanspruch geltend zu machen. Hier ist ein berechtigtes Interesse des Geschädigten zu bejahen.

Besondere Vorschriften gelten wiederum für die Übermittlung besonderer Arten personenbezogener Daten (vgl. § 3 Absatz 9).

Wie bereits dargelegt, gilt der Zweckbindungsgrundsatz auch bei der Übermittlung im nicht-öffentlichen Bereich. Weitere Besonderheiten im nicht-öffentlichen Bereich werden im Kapitel 3 erläutert.

Wann ist die Übermittlung ins Ausland zulässig?

Gesetzesbestimmungen: §§ 4b, 4c BDSG

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

Der Datenverkehr zwischen den Mitgliedstaaten der Europäischen Union – also innerhalb des europäischen Binnenmarktes – und mit den anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum im Anwendungsbereich des Unionsrechts ist genauso zu behandeln wie der inländische (vgl. § 4b Absatz 1).

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.

Wie ist das angemessene Datenschutzniveau festzustellen?

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

– 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 Absatz 3),

– durch die Europäische Kommission nach Art. 25 Absatz 6 der Richtlinie 95/46/EG (so bisher geschehen für Argentinien, Guernsey, Isle of Man, Jersey, Kanada, die Schweiz und Färöer).

– Ein Sonderweg wurde für den Datenverkehr mit den USA geschaffen. Es handelt sich um die sogenannten „Safe Harbor Principles“ („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.

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

Bedeutsam ist auch die Genehmigung der Übermittlung durch die zuständige Datenschutzaufsichtsbehörde (vgl. § 4c Absatz 2). Hierfür können die verantwortlichen Stellen auch auf Standardvertragsklauseln für die Übermittlung (Standard Contractual Clauses) zurückgreifen oder sich selbst verbindliche Unternehmensregeln (Binding Corporate Rules) genehmigen lassen.

2.8 Vorherige Kontrolle risikoreicher Datenverarbeitung (sog. Vorabkontrolle)

Gesetzesbestimmungen: §§ 4d Absatz 5 und 6, 4f und 4g BDSG

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

Beispielhaft – nicht abschließend – nennt das Gesetz zwei Fallgestaltungen, in denen die Vorabkontrolle notwendig ist:

– bei der Verarbeitung von personenbezogenen Daten besonderer Art (§ 3 Absatz 9),

– bei Verfahren, die dazu dienen, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens.

Die Vorabkontrolle muss in folgenden Fällen nicht durchgeführt werden:

– wenn eine gesetzliche Verpflichtung zur Durchführung der Datenverarbeitung besteht,

– wenn die Einwilligung des Betroffenen vorliegt,

– wenn die Erhebung, Verarbeitung oder Nutzung im Rahmen der Zweckbestimmung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses erfolgt.

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 Absatz 2 Satz 1 i.V.m. § 4e Satz 1).

Vorabkontrolle

Ist eine Vorabkontrolle durch das Gesetz vorgeschrieben, ist sie eine weitere Voraussetzung für die Zulässigkeit der Datenverarbeitung. Wurde eine notwendige Vorabkontrolle vollständig unterlassen, ist die Datenverarbeitung rechtswidrig. Das inhaltliche Votum des Datenschutzbeauftragten ist für die verantwortliche Stelle aber nicht bindend.

Im Rahmen einer Vorabkontrolle prüft der Datenschutzbeauftragte sowohl die rechtliche Zulässigkeit der beabsichtigten Verarbeitung als auch, ob die vorgesehenen technischen und organisatorischen Maßnahmen nach dem Stand der Technik ausreichend und angemessen sind. Er kann hierzu eine Risikoanalyse durchführen und ein Sicherheitskonzept erstellen.

2.9 Technische und organisatorische Sicherung des Datenschutzes

Gesetzesbestimmungen: §§ 3a, 9, 9a, 10, 42a BDSG

Je komplexer die Datenverarbeitungssysteme werden, desto wichtiger ist es, frühzeitig Datenschutzrisiken zu erkennen, technische und organisatorische Maßnahmen vorzusehen, die eine für den Betroffenen einfache und effiziente Möglichkeit zum Selbstschutz bieten, und Anreize zu schaffen, Datenschutz möglichst frühzeitig in technische Systeme zu integrieren.

Schon bei der Konzeption von IT-Systemen müssen Belange des Datenschutzes gewährleistet werden („Privacy by Design"). Dabei geht es in erster Linie darum, den Umfang der erhobenen und verarbeiteten personenbezogenen Daten auf ein Minimum zu beschränken. § 3a enthält die folgenden Vorgaben zur Datenvermeidung und Datensparsamkeit:

„Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert."

Zu einer datenschutzgerechten Technikgestaltung gehören auch entsprechende Voreinstellungen von IT-Systemen und elektronischen Diensten („Privacy by Default"). So sollte ein WLAN-Router nur mit voreingestellter Verschlüsselung ausgeliefert werden. Soziale Netzwerke im Internet sollten so konfiguriert sein, dass die Daten neuer Mitglieder nicht allgemein zugänglich sind.

Ein sehr wichtiger Bereich des Datenschutzes sind die **technischen und organisatorischen Maßnahmen**, die zum Schutz von personenbezogenen Daten getroffen werden müssen, um sie vor Missbrauch und Verarbeitungsfehlern zu sichern. Welche Maßnahmen notwendig sind, hängt sowohl von der Art der Daten ab, als auch von der Aufgabe, den organisatorischen Bedingungen, den räumlichen Verhältnissen, der personellen Situation und anderen Rahmenbedingungen der Verarbeitung. Das Gesetz verzichtet deshalb darauf, bestimmte einzelne Maßnahmen zwingend vorzuschreiben, sondern verlangt,

„die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführungen der Vorschriften dieses Gesetzes ... zu gewährleisten." (§ 9)

Welche Wirkung diese Maßnahmen im Bereich der automatisierten Verarbeitung haben müssen, legt das Gesetz in einer Anlage zu § 9 katalogmäßig fest (siehe Anhang 2). Die Maßnahmen müssen sich nach dem Stand der Technik richten und sind daher regelmäßig fortzuschreiben. Ziel dieser Maßnahmen ist das Erreichen bestimmter Schutzziele.

Schutzziele des technisch-organisatorischen Datenschutzes:

- Verfügbarkeit
  → Verfahren und Daten stehen zeitgerecht zur Verfügung und können ordnungsgemäß angewendet werden.

- Vertraulichkeit
  → Auf Verfahren und Daten darf nur befugt zugegriffen werden.

- Integrität
  → Daten aus Verfahren bleiben unversehrt, zurechenbar und vollständig.

- Transparenz
  → Erhebung, Verarbeitung und Nutzung personenbezogener Daten müssen mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden können.

- Unverkettbarkeit
  → Verfahren sind so einzurichten, dass deren Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können (technisch-organisatorische Gewährleistung der Zweckbindung).

- Intervenierbarkeit
  → Verfahren sind so zu gestalten, dass sie dem Betroffenen die Ausübung der ihm zustehenden Rechte wirksam ermöglichen.

Die technischen und organisatorischen Maßnahmen müssen als ein zusammenwirkendes Schutzsystem verstanden werden. Viele Maßnahmen des Datenschutzes wirken zugleich im Sinne einer Sicherung des Betriebsablaufs. Deshalb steht das Datenschutzkonzept in engem Zusammenhang mit sonstigen Sicherheitskonzepten.

Besondere Bedeutung erhält die sorgfältige Erarbeitung eines Datenschutzkonzepts im Zusammenhang mit der neu eingeführten **Pflicht zur Information bei Datenschutzpannen** gemäß § 42a. Danach müssen nicht-öffentliche Stellen, die personenbezogene Daten erheben, verarbeiten oder nutzen, im Falle des Verlusts von als besonders gefährdet eingestuften Daten die Betroffenen sowie die Aufsichtsbehörde hierüber informieren. Diese Vorgabe gilt gleichermaßen für Unternehmen, Vereine und Verbände und jedes ihnen gleichgestellte öffentlich-rechtliche Wettbewerbsunternehmen (z. B. städtisches Energieversorgungsunternehmen). Erfolgt diese Information nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig, droht nach § 43 Absatz 2 Nr. 7 regelmäßig ein Bußgeld.

Für die Einrichtung **automatisierter Verfahren zum Abruf personenbezogener Daten** durch Dritte sind besondere Anforderungen zu beachten. Sie sind nur zulässig, wenn sie unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen einerseits und der Aufgaben oder Geschäftszwecke der beteiligten Stellen andererseits angemessen sind. Hinzuweisen ist auch darauf, dass bei automatisierten Abrufverfahren eine Pflicht zur stichprobenweisen Protokollierung der Abrufe besteht (§ 10).

Immer wichtiger wird es, wettbewerbliche Anreize für Datenschutzmaßnahmen zu setzen, so dass besserer Datenschutz auch ökonomisch als Wettbewerbsvorteil begriffen werden kann. Mit dem sogenannten **„Datenschutzaudit"** könnten sowohl Anbieter von Datenverarbeitungssystemen und -programmen als auch verantwortliche Stellen ihre Datenschutzkonzepte sowie ihre technischen Einrichtungen mit einem datenschutzrechtlichen Gütesiegel versehen lassen und damit werben. Die Prüfung sollte durch unabhängige und zugelassene Gutachter erfolgen. Bisher gibt es kein bundesweites Datenschutzaudit nach § 9a. Die Regelung in § 9a läuft bisher leer, da ein Ausführungsgesetz fehlt, das alle weiteren Anforderungen an das Verfahren regelt. Derzeit wird darüber diskutiert, das Datenschutzaudit einer neu einzurichtenden „Stiftung Datenschutz" zu übertragen.

2.10 Der behördliche und betriebliche Beauftragte für den Datenschutz

Gesetzesbestimmungen: §§ 4f, 4g BDSG

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 Bundesbehörden müssen behördliche Beauftragte für den Datenschutz bestellen. Je nach Struktur der Stelle können mehrere Behörden auch einen gemeinsamen Datenschutzbeauftragten benennen. Bei den nicht-öffentlichen Stellen hängt die Verpflichtung zur Bestellung des oder der Beauftragten von der Größe der Stelle und der Zahl der mit der Verarbeitung personenbezogener Daten beschäftigten Arbeitnehmer ab. Die freiwillige Bestellung des oder der Beauftragten ist immer möglich. Bei der geschäftsmäßigen Datenverarbeitung zum Zweck der Übermittlung oder anonymisierten Übermittlung müssen immer Datenschutzbeauftragte bestellt werden.

Beispiel:
So müssen z. B. Auskunfteien oder Unternehmen des Adresshandels unabhängig von der Zahl der Beschäftigten eine/n betrieblichen Datenschutzbeauftragte/n bestellen. Das Gleiche gilt auch für ein Unternehmen, das geschäftsmäßig personenbezogene Daten zum Abruf aus dem Internet bereithält.

Dies gilt auch stets, wenn wegen besonders risikoreicher Datenverarbeitung eine Vorabkontrolle durchgeführt werden muss (siehe Kapitel 2.8). (Weitere Informationen hierzu finden Sie in unserer Broschüre „Der Datenschutzbeauftragte in Behörde und Betrieb“).

Der oder die Beauftragte für den Datenschutz gehört zwar zur jeweiligen Behörde oder zum Betrieb, hat jedoch nach dem Gesetz eine herausgehobene Stellung: Er oder sie ist dem Leiter der öffentlichen oder nicht-öffentlichen Stelle unmittelbar zu unterstellen und in der Ausübung seiner Fachkunde weisungsfrei. Damit kann ihm oder ihr niemand, auch nicht der Leiter oder die Leiterin der Stelle, vorschreiben, wie er oder sie datenschutzrechtliche Fragen bewertet.

Die Position der Datenschutzbeauftragten ist zuletzt durch die Einführung eines besonderen Kündigungsschutzes noch einmal gestärkt worden. Sie können – wenn sie selbst Beschäftigte der verantwortlichen Stelle sind – während der Bestellung bzw. bis ein Jahr nach Beendigung der Bestellung nur aus wichtigem Grund gekündigt werden, etwa bei einem Einstellungsbetrug oder beharrlicher Arbeitsverweigerung. Der Kündigungsschutz gilt jedoch nicht für freiwillig bestellte Datenschutzbeauftragte.

Die Leiterin oder der Leiter der Stelle ist nicht an das Votum des/der internen Datenschutzbeauftragten gebunden. Damit bleibt die Letztverantwortung für die Datenverarbeitung bei der Unternehmensleitung.

Um der hohen Bedeutung der Datenschutzbeauftragten für einen wirkungsvollen Datenschutz Rechnung zu tragen, darf für diese Aufgabe nur bestellt werden, wer die erforderliche „Fachkunde und Zuverlässigkeit" besitzt. Der bzw. die Datenschutzbeauftragte muss also sowohl die technische als auch die rechtliche Seite der Aufgaben kennen und gute Kenntnisse in allen Bereichen haben, die für die jeweilige Organisation von Bedeutung sind. Die verantwortliche Stelle ist verpflichtet, dem bzw. der Datenschutzbeauftragten zum Erhalt der Fachkunde die Teilnahme an Schulungs- und Fortbildungsveranstaltungen zu ermöglichen und hierfür die Kosten zu übernehmen.

Die behördlichen und betrieblichen Datenschutzbeauftragten sind gesetzlich zur Verschwiegenheit verpflichtet. Über die Identität des Betroffenen (Beschwerdeführers) oder Umstände, die Rückschlüsse hierüber erlauben, dürfen sie keine Auskünfte geben. Eine Ausnahme gilt nur, wenn die betroffene Person sie von seiner Verschwiegenheitsverpflichtung befreit.

Die Aufgaben der behördlichen und betrieblichen Datenschutzbeauftragten sind vielfältig. Sie müssen

- 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.

2.11 Datenverarbeitung im Auftrag

Gesetzesbestimmung: § 11 BDSG

Privatwirtschaft wie auch öffentliche Verwaltung führen Teile ihrer Aufgaben nicht mehr selbst aus, sondern betrauen damit Dritte. Entschließt sich eine Stelle zum Outsourcing solcher Tätigkeiten, die auch die Erhebung, Verarbeitung und Nutzung personenbezogener Daten beinhalten, muss sie dabei verschiedene rechtliche, technische und organisatorische Voraussetzungen erfüllen. § 11 regelt die sogenannte Auftragsdatenverarbeitung.

Beispiele für die Datenverarbeitung im Auftrag:

- *Betrieb eines Rechenzentrums im Auftrag*
- *Entsorgung von Datenträgern*
- *technischer Betrieb einer virtuellen Poststelle*

Werden dem Auftragnehmer personenbezogene Daten zu diesem Zweck überlassen, findet datenschutzrechtlich gesehen keine Übermittlung statt, da der Auftragnehmer nicht Dritter ist. Gegenüber den Bürgerinnen und Bürgern bleibt der Auftraggeber (also die Stelle, um deren Aufgabe es geht) voll dafür verantwortlich, dass mit ihren personenbezogenen Daten rechtmäßig umgegangen wird.

Dies setzt voraus, dass

- der Auftraggeber einen schriftlichen Auftrag erteilen muss (was genau schriftlich geregelt werden muss, legt § 11 Absatz 2 detailliert fest),

- der Auftragnehmer nur im Rahmen der Weisungen seines Auftraggebers tätig werden darf und

- der Auftraggeber die erforderlichen Maßnahmen zur Datensicherheit vorgeben muss.

Der Auftraggeber muss sich vor Beginn der Datenverarbeitung und sodann regelmäßig über die Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugen und das Ergebnis dieser Überprüfung dokumentieren.

Im Regelfall wird sich der Auftraggeber vor Ort davon vergewissern, dass seine Vorgaben, insbesondere im Hinblick auf die technisch-organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes, ein-

gehalten werden. Es ist jedoch möglich, diese Aufgabe gegebenenfalls an vertrauenswürdige Dritte (etwa durch unabhängige Sachverständige oder Wirtschaftsprüfungsgesellschaften, die kein eigenes Interesse an der Bewertung haben) zu delegieren, welche die Einhaltung der Vorgaben bescheinigen. Letzteres kommt insbesondere dann in Betracht, wenn die Auftragsdatenverarbeitung im Ausland durchgeführt wird.

Werden Aufträge an Auftragnehmer erteilt, die ihren Sitz im Europäischen Wirtschaftsraum haben und die Datenverarbeitung dort ausführen, gelten dieselben Vorgaben wie für inländische Auftragnehmer. Bei der Auftragsvergabe an Auftragnehmer in sonstigen Drittstaaten sind besondere Bedingungen zu beachten.

2.12 Die wichtigsten Änderungen im Überblick

Durch die zum 1. September 2009, 1. April 2010 sowie 11. Juni 2010 in Kraft getretenen Novellen ist eine Reihe von Änderungen eingetreten.

Nachfolgend soll nur schlagwortartig eine kurze Übersicht gegeben werden:

- präzisere Definition der Grundsätze der Datenvermeidung und Datensparsamkeit, § 3a

- Stärkung der betrieblichen Datenschutzbeauftragten, § 4 f

- Regelungen, unter welchen Voraussetzungen personenbezogene Daten an Auskunfteien übermittelt werden dürfen, § 28a, einschließlich in Teilbereichen Regelungen, inwieweit personenbezogene Daten für die Bonitätsbewertung herangezogen werden dürfen, § 6, 28a Absatz 2 Satz 4, 28 Absatz 3

- Regelungen, unter welchen Voraussetzungen Scoreverfahren im Rahmen von Vertragsverhältnissen eingesetzt werden dürfen, § 28b

- mehr Transparenz:
  - Im Falle automatisierter Einzelfallentscheidungen muss der Betroffene zukünftig umfassender informiert werden, bei ihn beeinträchtigenden Entscheidungen auf Verlangen auch über die wesentlichen Gründe aufgeklärt werden (§ 6a).
  - Bei Ablehnung eines Verbraucherdarlehensvertrages aufgrund von Bonitätsauskünften einer Auskunftei muss der Verbraucher über diese Auskunft unterrichtet werden (§ 29 Absatz 7).

  - Einmal im Jahr müssen insbesondere Auskunfteien auf Antrag kostenlos Auskunft zu den bei ihnen gespeicherten personenbezogenen Daten geben (§ 34 Absatz 8).
  - Beim Einsatz von Scoringverfahren hat der Betroffene einen Anspruch darauf, dass ihm das Zustandekommen seines Scorewertes einzelfallbezogen und nachvollziehbar erläutert wird (§§ 28 b, 34).
  - Informationspflicht bei Datenschutzpannen (§ 42 a).

- schärfere Anforderungen bei der Auftragsdatenverarbeitung (§ 11).

- Einschränkungen bei postalischer Werbung und Adresshandel (§ 28 Absatz 3). Grundsätzlich soll vom Betroffenen eine Einwilligung eingeholt werden. Es gibt jedoch zahlreiche Ausnahmen.

- Verbot der Koppelung des Abschlusses eines Vertrages mit der Einwilligung in die Datenverarbeitung zu Werbezwecken, (§ 28 Absatz 3 b).

- Privilegierung der Markt- und Meinungsforschung bei der Nutzung von Adressdaten (§ 30 a). Eine Datenerhebung, -verarbeitung und -nutzung ist grundsätzlich auch ohne Einwilligung des Betroffenen möglich.

- Einführung einer eigenen Norm zum Arbeitnehmerdatenschutz, (§ 32) einschließlich einer Definition des Begriffs „Beschäftigte“ (§ 3 Absatz 11).

- bessere Sanktionsbefugnisse:
  - die Bußgeldtatbestände wurden erweitert, die Bußgelder erhöht (§ 43).
  - Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich können bei materiell-rechtlichen Verstößen Anordnungen erlassen, etwa Auflagen oder sogar Verbote aussprechen (§ 38 Absatz 5).

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

3.1 Rechtsgrundlagen der Datenverarbeitung

Gesetzesbestimmungen: §§ 28, 29, 30a BDSG

Das Gesetz unterscheidet zwischen der Datenerhebung und -verarbeitung für eigene Geschäftszwecke in § 28 und der geschäftsmäßigen Erhebung und Verarbeitung zum Zwecke der Übermittlung in § 29.

Typischerweise handelt es sich im ersteren Fall um ein Unternehmen, das bei seinen eigenen Kunden im Rahmen der Vertragsbeziehung Daten erhebt und diese zur Erfüllung der Vertragszwecke nutzt. Dies ist ohne ausdrückliche Einwilligung der Betroffenen zulässig.

Beispiel:
Ein Möbelhändler erhebt bei einem Kunden im Rahmen eines Verkaufs Name und Anschrift, um die Ware liefern zu können. Der Kunde zahlt mit der ec-Karte, der Händler nutzt die so gewonnenen Kontoinformationen ausschließlich zum Zwecke des Bankeinzugs.

Die Tätigkeit von Adresshändlern und Auskunfteien ist hingegen ein Fall der geschäftsmäßigen Datenerhebung und -verarbeitung zum Zwecke der Übermittlung.

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 oder dem Adresshandel dient (s. dazu die nachfolgenden Kapitel).

Auch die Markt- und Meinungsforschung gehört grundsätzlich in diesen Bereich. Die Datenverarbeitung wurde jedoch vom Gesetzgeber in einer eigenen Vorschrift geregelt (vgl. § 30 a). Eine Einwilligung der Betroffenen in die Datenverarbeitung ist danach nicht erforderlich. Um die Interessen der Betroffenen zu wahren, müssen die Daten anonymisiert werden, sobald dies nach dem Zweck des Forschungsvorhabens möglich ist. Bis zur Anonymisierung sind die Merkmale, die eine Herstellung des Personenbezugs ermöglichen, zudem gesondert zu speichern. Darüber hinaus dürfen die Daten nur zweckgebunden für das Forschungsvorhaben verwendet werden.

Die Nutzung von personenbezogenen Daten zu Zwecken der postalischen Werbung und des Adresshandels ist abschließend in § 28 Absatz 3 geregelt.

3.2 Werbung und Adresshandel

Gesetzesbestimmung: § 28 BDSG

Seit dem 1. September 2009 dürfen personenbezogene Daten grundsätzlich nur mit Einwilligung des Betroffenen zu Zwecken der Werbung und des Adresshandels weitergegeben werden. Von diesem Grundsatz gibt es – bezogen auf postalische Direktwerbung – jedoch zahlreiche Ausnahmen.

Ohne Einwilligung dürfen personenbezogene Daten zu Zwecken der Werbung oder des Adresshandels verarbeitet oder genutzt werden,

- wenn der Betroffene anhand der Werbung erkennen kann, welches Unternehmen seine Adressdaten hierfür weitergegeben hat. Dazu müssen Herkunft und Weitergabe der Adressdaten dokumentiert werden. Bereits aus der Werbung selbst muss für den Betroffenen erkennbar sein, wer seine Daten erstmalig weitergegeben hat. Diese Stelle muss dem Betroffenen dann auf Nachfrage mitteilen können, an wen sie seine Daten zu Werbezwecken in den letzten zwei Jahren weitergegeben hat.

- wenn Unternehmen ihre eigenen Kunden bewerben. Nutzen dürfen sie hierfür sogenannte Listdaten, die sie beim Betroffenen selbst erhoben oder aus allgemein zugänglichen Quellen (etwa Telefonbüchern) entnommen haben. Jedoch dürfen nicht unterschiedslos alle Kundendaten für Werbezwecke herangezogen werden, sondern nur ein bestimmter Katalog listenmäßig oder sonst zusammengefasster Daten. Derartig zusammengefasst werden dürfen nur Angaben zu Name, Titel, akademischem Grad, Anschrift und Geburtsjahr, Berufs-, Branchen- oder Geschäftsbezeichnung sowie eine Angabe, die die Zugehörigkeit des Betroffenen zu einer bestimmten Personengruppe charakterisiert (z.B. Versandhauskunde).

Das Gesetz sieht für die von den Änderungen betroffenen Unternehmen eine Übergangsfrist von drei Jahren vor. Für Daten, die vor dem 1. September 2009 erhoben wurden, gilt die alte Rechtslage zunächst fort, d. h.:

Daten, insbesondere zu Name, Anschrift, Geburtsjahr, Beruf sowie akademische Grade und Titel (die sogenannten Listdaten), können ohne Einwilligung des Betroffenen weiter wie bisher genutzt werden, und zwar

– für Zwecke der Markt- oder Meinungsforschung bis zum 31. August 2010,

– für Zwecke der Werbung bis zum 31. August 2012.

Werbewiderspruch

Sie haben das Recht, der Zusendung persönlich an Sie adressierter Werbung zu widersprechen. Auf dieses Recht müssen Sie hingewiesen werden, wenn Sie Werbung zugesandt bekommen. Es sollte also bereits auf dem Werbeschreiben vermerkt sein, wo und wie Sie den Widerspruch einlegen können.

Dieses Nutzungsverbot in Form eines Widerspruchs können Sie auch schon bei der erstmaligen Bekanntgabe Ihrer persönlichen Daten gegenüber dem Geschäfts- oder Vertragspartner aussprechen, z.B. durch einen entsprechenden Vermerk auf dem Antrags- bzw. Vertragsformular. Der Widerspruch ist aber auch zu einem späteren Zeitpunkt möglich. Er kann auch bei den Stellen eingelegt werden, denen die Daten übermittelt worden sind. Für den Widerspruch, der keiner weiteren Begründung bedarf, reicht folgende Formulierung:

„Ich widerspreche der Nutzung oder Übermittlung meiner Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung (§ 28 Abs. 4 Bundesdatenschutzgesetz).“

Robinsonliste

Personen, die keine Werbung per Briefpost wünschen, können sich in die sogenannte Robinsonliste aufnehmen lassen. Hierzu kann ein Aufnahmeformular unter folgender Anschrift angefordert werden:

Deutscher Dialogmarketing Verband e.V. (DDV)
- Robinson-Liste -
Postfach 14 01
71243 Ditzingen
Telefon: (07156) 95 10 10

Die Formulare werden auch im Internet als PDF-Datei zum Herunterladen angeboten: http://www.direktmarketing-info.de/

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

Ferner gibt die Deutsche Telekom AG 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

DeTeMedien GmbH
Wiesenhüttenstr. 18
60329 Frankfurt
Telefon: (069) 26 82-0
Fax: (069) 26 82-11 01

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.

3.3 Die Tätigkeit von Auskunfteien

Gesetzesbestimmungen: §§ 28a, 29 BDSG

Ein Unternehmen darf unter den Voraussetzungen von § 29 geschäftsmäßig personenbezogene Daten erheben und verarbeiten, um diese Daten Dritten zu übermitteln. Dies geschieht insbesondere bei Auskunfteien, die anderen Unternehmen Angaben zur Kreditwürdigkeit von Privatpersonen verkaufen.

Auskunfteien erheben und speichern Angaben zu vertragsgemäßem wie nicht-vertragsgemäßem Verhalten.

§ 28a legt fest, welche personenbezogenen Daten zu nicht-vertragsgemäßem Verhalten in Bezug auf eine Forderung an Auskunfteien übermittelt werden und also auch von Auskunfteien erhoben und verarbeitet werden dürfen.

Folgende personenbezogene Daten dürfen an eine Auskunftei übermittelt werden:

- Forderungen, die durch rechtskräftige Urteile festgestellt worden sind
- Forderungen im Rahmen von Insolvenzverfahren
- ausdrücklich anerkannte Forderungen
- jede Art der Forderung, wenn sie mindestens zweimal schriftlich gemahnt worden sind, auf die Einmeldung hingewiesen wurden und Sie die Forderung nicht bestritten haben.
- jede Art von Forderung, die Ihren Vertragspartner zur fristlosen Kündigung berechtigt, wenn Sie vorher über die Einmeldung bei einer Auskunftei informiert worden sind

Zusätzlich dürfen Auskunfteien von Banken und anderen Kreditinstituten weitere Informationen erhalten, nämlich Angaben über Girokontenverträge, laufende Kredite, beantragte Hypotheken oder andere Bankgeschäfte. Nur wenn ein Girokonto auf Guthabenbasis geführt wird, darf weder diese Information, noch überhaupt eine Angabe zu diesem Girokontoverhältnis (Ablauf, Dauer, Beendigung) an eine Auskunftei übermittelt werden.

Sie haben das Recht, von Auskunfteien Auskunft zu den über Sie gespeicherten Daten zu erhalten (s. Kapitel 4.1.).

3.4 Scoring

Gesetzesbestimmungen: §§ 28b, 34 BDSG

Viele Auskunfteien ermitteln für ihre Vertragspartner einen sogenannten Scorewert (score = Punktzahl) über Privatpersonen. Hierbei handelt es sich um einen Wert, der auf der Grundlage eines mathematisch-statistischen Verfahrens aus den bei der Auskunftei vorhandenen Angaben errechnet wird und eine Aussage über die Wahrscheinlichkeit des künftigen Zahlungsverhaltens der Betroffenen und damit über ihre Kreditwürdigkeit enthalten soll. Dem Empfänger dieser Information bleibt

es überlassen festzulegen, wie diese Risikoprognose in Bezug auf sein Geschäftsinteresse zu bewerten ist.

Der Gesetzgeber hat den Einsatz von Scorewerten nicht verboten. Werden diese jedoch eingesetzt, um zu entscheiden, ob und zu welchen Bedingungen ein Vertrag mit Ihnen abgeschlossen werden soll, dann müssen bestimmte Vorgaben beachtet werden.

- Die Seriosität von Scorewerten muss wissenschaftlich nachgewiesen worden sein.
- Wenn eine Auskunftei den Scorewert berechnet, darf sie nicht automatisch ihren ganzen Datenbestand zugrunde legen.
- Ein Scorewert darf nicht überwiegend auf der Grundlage von Anschriftendaten ermittelt werden.
- Wenn Anschriftendaten verwendet werden, muss der Betroffene hierüber vorher unterrichtet worden sein.

Wenn Anschriftendaten für einen Scorewert herangezogen werden, spricht man von Geoscoring. Dies bedeutet, dass etwa die Bonität davon abhängig gemacht wird, in welcher Wohngegend jemand lebt. Verboten ist es, einen Score im Wesentlichen auf die Wohngegend zu stützen, also zur Berechnung des Scorewertes keine weiteren oder nur solche Angaben hinzuzuziehen, die keinen wesentlichen Einfluss auf die Entscheidung haben.

Jede Stelle, die Scorewerte einsetzt oder errechnet und an Dritte weitergibt, muss Ihnen erläutern, welche Scorewerte zu Ihrer Person gespeichert sind, an wen welcher Scorewert übermittelt worden ist und wie dieser Scorewert zustande gekommen ist.

Der Scorewert muss Ihnen verständlich, einzelfallbezogen und nachvollziehbar erklärt werden, damit Sie Ihre Rechte sachgerecht ausüben, mögliche Fehler in der Berechnungsgrundlage aufdecken und Abweichungen von den automatisiert gewonnenen typischen Bewertungen des zugrunde liegenden Lebenssachverhalts darlegen können.

Zur Verwendung von Scorewerten im Rahmen automatisierter Einzelentscheidungen vergleiche Kapitel 4.5.

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 Bundesdatenschutzgesetz an zwei Stellen unter der Überschrift „Rechte des Betroffenen" – zum einen als Rechte gegenüber öffentlichen Stellen in den §§ 19ff., zum anderen gegenüber nicht-öffentlichen Stellen in den §§ 33 ff (zur Definition des Begriffes „Betroffener" siehe § 3 Absatz 1, bzw. in Kapitel 6).

Aber auch an anderer Stelle trifft das Bundesdatenschutzgesetz Regelungen für bestimmte Bereiche, z.B. für die Videoüberwachung, bei denen sich aus den Pflichten für die verantwortlichen 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 Bundesdatenschutzgesetz 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 Bundesdatenschutzgesetzes 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?

- 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 (Kapitel 6). Außerdem können Ihnen die Datenschutzkontrollinstitutionen weiterhelfen (Anhänge 5 und 6).

Was kostet eine Auskunft?

Grundsätzlich brauchen Sie für die Auskunft nichts zu bezahlen.

Von Auskunfteien und anderen Stellen, die Ihre Daten geschäftsmäßig zum Zwecke der Übermittlung speichern (Kapitel 3.3 und 3.4), haben Sie das Recht, einmal im Kalenderjahr kostenlos Auskunft zu erhalten. Für jede weitere Auskunft kann jedoch ein Entgelt verlangt werden, wenn die Auskunft gegenüber Dritten wirtschaftlich genutzt werden kann (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.

Gegebenenfalls können Auskünfte auch elektronisch, etwa per E-Mail, erteilt werden. Dabei ist allerdings zu beachten, dass mit der elektroni-

schen Übermittlung gegebenenfalls zusätzliche Risiken verbunden sind. Deshalb achten Sie darauf, dass eine verschlüsselte Datenübermittlung gewährleistet ist.

Was ist an Besonderheiten zu beachten?

Bei öffentlichen Stellen

- 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, insbesondere Auskunfteien

- 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.
- Von allen Stellen, die Scorewerte einsetzen oder errechnen, haben Sie das Recht zu erfahren, welche Scorewerte zu Ihrer Person gespeichert sind, an Dritte übermittelt worden sind und wie diese Scorewerte zustande gekommen sind. Der Scorewert muss Ihnen verständlich, einzelfallbezogen und nachvollziehbar erklärt werden. Näheres hierzu können Sie im Kapitel 3.4 „Scoring“ nachlesen. Wenn Sie Ihren Auskunftsanspruch geltend machen, darf sich dies nicht negativ auf Ihren Scorewert auswirken.

In welchen Fällen hat man keinen Anspruch auf Auskunft?

Öffentliche Stellen dürfen die Auskunft verweigern, soweit

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

– die Auskunft die öffentliche Sicherheit oder Ordnung gefährden würde 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), 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 Absatz 7 i.V.m. § 33 Absatz 2 Satz 1 Nr. 2, 3 und 5–7).

Was tun, wenn die Auskunft verweigert wird?

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

Soweit die auskunftspflichtige Stelle nicht oder 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 verantwortliche Stelle auch verpflichtet zu begründen, aufgrund welcher gesetzlichen Bestimmung und aufgrund welcher Tatsachen sie eine Auskunft verweigert oder beschränkt. Eine solche Begründung ist nur entbehrlich, wenn sonst der mit der Auskunftsverweigerung verfolgte Zweck (z.B. laufende polizeiliche Ermittlungen nicht zu behindern) gefährdet würde.

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 Kapitel 4.8). Sie haben außerdem die Möglichkeit einer gerichtlichen Klage.

4.2 Das Einsichtsrecht in das Verfahrensverzeichnis

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

Die öffentlichen Stellen des Bundes haben ebenso wie die verantwortlichen Stellen im nicht-öffentlichen Bereich eine Übersicht über ihre automatisierten Verarbeitungen personenbezogener Daten zu führen. Diese Übersicht kann von jedermann unentgeltlich eingesehen werden.

Es ist Aufgabe der behördlichen oder betrieblichen Datenschutzbeauftragten, auf Antrag die Angaben in dem Verfahrensverzeichnis den Antragstellern in geeigneter Weise verfügbar zu machen. Auch nicht-öffentliche Stellen ohne betrieblichen Datenschutzbeauftragten müssen eine entsprechende Übersicht führen und zur Einsicht bereithalten. 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 insbesondere um folgende Angaben:

- Name oder Firma der verantwortlichen Stelle,
- Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
- Anschrift der verantwortlichen Stelle,
- Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,
- eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,

- Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
- Regelfristen für die Löschung der Daten,
- eine geplante Datenübermittlung in Drittstaaten.

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

Hinweis: Das Verzeichnis enthält keine Angaben über die konkret gespeicherten Datensätze. Es kann ihm also nicht entnommen werden, ob überhaupt und, wenn ja, welche Daten gerade über Sie oder eine andere Person gespeichert sind. Das Verzeichnis kann allerdings Anhaltspunkte dafür liefern, gegenüber welcher Stelle Sie Ihr Recht auf Auskunft (Kapitel 4.1) geltend machen wollen.

Ausnahmen:

Nicht öffentlich einsehbar sind die Verzeichnisse folgender Behörden:

– Verfassungsschutzbehörden,

– Bundesnachrichtendienst,

– Militärischer Abschirmdienst,

– andere Behörden des Bundesministeriums 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

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. Unternehmen, die geschäftsmäßig personenbezogene Daten verarbeiten, haben die Betroffenen ebenfalls erst bei der erstmaligen Übermittlung zu benachrichtigen. Alle anderen nicht-öffentlichen Stellen müssen bereits bei der ersten Speicherung benachrichtigen.

Die Benachrichtigung muss umfassen

- die Angabe der verantwortlichen Stelle (öffentliche Stelle bzw. Firma, Anschrift),
- die Tatsache, dass erstmals Daten über die Person, die benachrichtigt wird, gespeichert oder übermittelt werden,
- 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.

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 Absatz 2, 33 Absatz 2). Im öffentlichen Bereich hat die Benachrichtigung nur eine

geringe Bedeutung, weil sie auch dann entfallen kann, wenn die Speicherung oder Übermittlung der personenbezogenen Daten durch Gesetz ausdrücklich vorgesehen ist.

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. Geschätzte Daten (etwa die Schätzung des Alters eines Betroffenen) müssen als solche deutlich gekennzeichnet werden.

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?

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); soweit es sich um Daten über erledigte Sachverhalte handelt, muss bereits zum Ende des dritten Kalenderjahres nach der ersten Speicherung die Löschverpflichtung überprüft werden.

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,

  Beispiel:
  Handels- oder steuerrechtliche Aufbewahrungspflichten können einer Löschung ebenso entgegenstehen wie z. B. Registraturvorschriften einer Behörde.

– 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. Die Tatsache dieser Sperrung darf dann gleichfalls nicht übermittelt werden.

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.

Zusätzlich schreibt das Gesetz vor, dass gesperrte Daten nur ausnahmsweise und nur dann für die genannten Zwecke übermittelt oder genutzt werden dürfen, wenn dies auch ohne Sperrung erlaubt wäre.

4.4 Das allgemeine Widerspruchsrecht

Gesetzesbestimmungen § 20 Absatz 5, 35 Absatz 5 BDSG

Wann greift das Widerspruchsrecht?

Als Betroffener haben Sie das Recht, unter bestimmten Voraussetzungen sogar einer rechtmäßigen Datenverarbeitung zu widersprechen. Für den öffentlichen Bereich ist das in § 20 Absatz 5, für den nicht-öffentlichen Bereich in § 35 Absatz 5 geregelt.

Der Widerspruch ist begründet,

– sofern besondere Umstände in der Person des Betroffenen vorliegen,

– das schutzwürdige Interesse des Betroffenen das Interesse der verantwortlichen Stelle an der Erhebung, Verarbeitung oder Nutzung der entsprechenden personenbezogenen Daten überwiegt.

Beispiel:
Ein gefährdeter Zeuge in einem Strafverfahren kann der Weitergabe seiner Daten durch eine Auskunftei widersprechen. Eine melderechtliche Auskunftssperre wegen einer besonderen Gefährdung von Leib und Leben kann hierfür ein Indiz sein.

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

Auch wenn die gesetzlichen Vorschriften kein explizites Widerspruchsrecht in Fällen vorsehen, in denen eine Abwägung berechtigter Interes-

sen der verantwortlichen Stelle mit schutzwürdigen Belangen des Betroffenen erfolgen muss (etwa bei der Verarbeitung personenbezogener Daten durch nicht-öffentliche Stellen gem. §§ 28, 29 – vgl. Kapitel 3), kann es sinnvoll sein, Widerspruch einzulegen, um die eigenen berechtigten Interessen geltend zu machen. Die verantwortliche Stelle hat den Widerspruch in den Abwägungsprozess einzubeziehen.

Beispiel:
Aufnahme der Anschrift eines Vereinsmitglieds in eine allen Mitgliedern zugängliche Mitgliederliste

Zu den Besonderheiten des Werbewiderspruchs vgl. Kapitel 3.2 „Werbung und Adresshandel".

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 Bundesdatenschutzgesetz in der Regelung zur automatisierten Einzelentscheidung in § 6a 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. 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 insbesondere bei der Kreditvergabe verwandt wird (vgl. Kapitel 3.4).

Beispiel:
Wenn für die Entscheidung, ob und zu welchen Bedingungen ein Vertrag zustande kommt, die Bewertung eines Persönlichkeitsmerkmals wie der Kreditwürdigkeit durch ein Computerprogramm vorgenommen wurde, dann muss

grundsätzlich immer ein Mensch vor die eigentliche Vertragsentscheidung vorgeschaltet werden. Ein Sachbearbeiter muss das automatisierte Ergebnis im Einzelfall überprüfen und die Entscheidung selbst treffen können, die auch von der Vorgabe des Computers abweichen können muss.

Nur in Ausnahmefällen darf von dem Verbot der automatisierten Einzelentscheidung abgewichen werden. So muss insbesondere bei negativen Entscheidungen das Verfahren für den Betroffenen transparent sein, so dass er nachträglich seine Rechte wahren kann.

Das Verbot der automatisierten Entscheidung gilt daher nicht,

- wenn die Entscheidung im Rahmen eines Vertragsverhältnisses oder sonstigen Rechtsverhältnisses ergeht und dem Anliegen des Betroffenen stattgegeben wird oder

- 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 informiert wird und ihm auf Verlangen die wesentlichen Gründe für diese Entscheidung mitgeteilt werden.

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.

Als weitere Besonderheit bei automatisierten Einzelentscheidungen bezieht sich das Auskunftsrecht des Betroffenen auch auf den logischen Aufbau des Verfahrens (vgl. § 6a Absatz 3).

4.6 Die Rechte beim Einsatz von Videoüberwachung

Gesetzesbestimmung: § 6b BDSG

Die Regelung 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, z. B. Kaufhäuser, Bahnhöfe oder auch Einkaufspassagen. § 6 b gilt nicht für die Beobachtung von Beschäftigten in Unternehmen oder Behörden in Bereichen, die der Öffentlichkeit nicht zugänglich sind. In diesem Falle ist ausschließlich das für die Beschäftigten geltende Datenschutzrecht anzuwenden.

Beispiel:
Für die Videoüberwachung der öffentlich zugänglichen Verkaufsräume eines Supermarktes ist § 6 b anzuwenden. Dies schließt auch den Bürgersteig im unmittelbaren Eingangsbereich des Marktes ein. Für die den Kunden nicht zugänglichen Bereiche, z.B. Lager- oder Technikräume gilt die Vorschrift hingegen nicht.

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.

Ist danach die Videoüberwachung erforderlich, müssen die mit der Videoüberwachung verfolgten Zwecke gegen die schutzwürdigen Interessen der von der Überwachung Betroffenen abgewogen werden. Ergeben sich hier Anhaltspunkte, dass schutzwürdige Interessen der Betroffenen überwiegen, ist die Videoüberwachung ebenfalls unzulässig. Nicht zulässig ist etwa die Überwachung des weiteren Umfelds eines Betriebs oder einer Behörde zur Wahrung des Hausrechts. Die heimliche Beobachtung öffentlich zugänglichen Raums ist grundsätzlich unzulässig.

Die Videoüberwachung muss durch geeignete Maßnahmen kenntlich gemacht werden. Da damit gerechnet werden muss, dass Menschen verschiedener Nationalitäten erfasst werden, sollten die Hinweisschilder mehrsprachig sein. Als Alternative kommt auch die Verwendung von Piktogrammen in Frage. Die jeweiligen Anforderungen müssen nach der Lage im Einzelfall beurteilt werden.

Die weitere Verarbeitung oder Nutzung von Videoaufnahmen (Speicherung/Auswertung), ist nur zulässig, soweit dies jeweils erforderlich ist. Kontrollfrage: Genügt nicht die einfache Beobachtung? Auch müssen erneut die schutzwürdigen Interessen des Betroffenen mit der geplanten Verarbeitung oder Nutzung im Rahmen einer Vorabkontrolle (Kapitel 2.8) abgewogen werden.

Wenn die durch Videoüberwachung erhobenen Daten einer bestimmten Person zugeordnet werden, muss diese Person über die Verarbeitung oder Nutzung entsprechend §§ 19a und 33 benachrichtigt werden. Nur so kann gewährleistet werden, dass diese von der Überwachung und der anschließenden Auswertung Kenntnis erhält und selbst für die Wahrung ihrer Rechte eintreten kann.

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 Das Recht Anrufung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sowie 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 und die Informationsfreiheit wenden. Als unabhängige Beschwerdeinstanz mit umfassenden Kontrollbefugnissen (vgl. Kapitel 1) geht der Bundesbeauftragte den Beschwerden 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 die Landesbeauftragten für den Datenschutz und andere Datenschutzaufsichtsbehörden anrufen, wenn Sie Ihre Rechte in deren Zuständigkeitsbereich verletzt sehen. Die örtliche Zuständigkeit für Unternehmen und andere nicht-öffentliche Stellen richtet sich nach dem Sitz der nicht-öffentlichen Stelle.

Die Kontaktdaten der Datenschutzkontrollinstitutionen finden Sie in den Anhängen 5 und 6 oder im Internet unter www.datenschutz.bund.de.

Da das Bundesdatenschutzgesetz im Bereich der **Kirchen und bei kirchlichen Einrichtungen** nicht gilt (s. auch Kapitel 2.3), haben die Evangelische Kirche in Deutschland, die Evangelischen Landeskirchen und die Bistümer der Katholischen Kirche in Deutschland eigene Datenschutzbeauftragte bestellt.

Weitere Informationen sowie die Links zu den kirchlichen Datenschutzbeauftragten finden Sie im Internet-Angebot des BfDI (www.datenschutz.bund.de) unter Themen/BDSG/Einzelfragen

Die Einhaltung der datenschutzrechtlichen Vorschriften bei den **öffentlich-rechtlichen Rundfunkanstalten** (die in der ARD zusammengeschlossenen Landesrundfunkanstalten, das ZDF und DeutschlandRadio) sowohl im journalistisch-redaktionellen als auch im Verwaltungsbereich wird von besonderen Rundfunkdatenschutzbeauftragten kontrolliert. Lediglich beim Hessischen Rundfunk, beim Rundfunk Berlin-Brandenburg und bei Radio Bremen wird der Verwaltungsbereich von den dortigen Landesbeauftragten für den Datenschutz kontrolliert. Zum Verwaltungsbereich gehört vor allem der Datenschutz bei der Erhebung der Rundfunkgebühren durch die Rundfunkanstalten bzw. die von diesen beauftragte Gebühreneinzugszentrale (GEZ). Anschriften und Telefonnummern der **Rundfunkbeauftragten für den Datenschutz** finden Sie in Anhang 7.

4.8 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. Diese Schadensersatzverpflichtung gilt sowohl für öffentliche als auch für nicht-öffentliche Stellen.

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 und muss zivilrechtlich durchgesetzt werden.

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.

Öffentliche Stellen haften – auch unabhängig von einem Verschulden – bis zu einem Höchstbetrag von 130.000 Euro (Gefährdungshaftung).

Auch bei der verschuldensunabhängigen Haftung gibt es bei schweren Persönlichkeitsverletzungen einen Schmerzensgeldanspruch.

5 Seien Sie Ihr eigener Datenschutzbeauftragter!

Zum Schutz Ihrer Privatsphäre können Sie selbst beitragen, denn Datenschutzaufsichtsbehörden können nicht überall sein. Gerade bei der Durchsetzung datenschutzfreundlicher Standards im globalen Datenaustausch über das Internet kommt es vielfach auf den aufmerksamen und kritischen Netzbürger an.

Datenschutz durch Technik umfasst auch Möglichkeiten des Selbstschutzes für den Einzelnen (vgl. Kapitel 2.2 und 2.9). Sorgen Sie für die Sicherheit und Vertraulichkeit Ihrer Daten im Internet, indem Sie die Möglichkeiten der 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. Eine aktuelle Informationsquelle hierfür sind das Internetangebot des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (www.datenschutz.bund.de) oder das „Virtuelle Datenschutzbüro“, das von vielen Datenschutzbehörden gemeinsam betrieben wird (www.datenschutz.de).

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 per-

sönliche Interessen zu erfahren. Das können auch die „Haushaltsumfrage“ eines Marktforschungsunternehmens oder die Kundenkarte sein, die Aufschluss über Ihr Konsumverhalten geben. Sie bestimmen mit, 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 oder ohne Not darauf zu verzichten.

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, 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 gespeicherter personenbezogener 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; Dritte sind nicht

– 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.

Beschäftigte sind

1. Arbeitnehmerinnen und Arbeitnehmer,

2. zu ihrer Berufsausbildung Beschäftigte,

3. Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden),

4. in anerkannten Werkstätten für behinderte Menschen Beschäftigte,

5. nach dem Jugendfreiwilligendienstegesetz Beschäftigte,

6. Personen, die wegen ihrer wirtschaftlichen Unselbstständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,

7. Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist,

8. Beamtinnen, Beamte, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende.

Anhang 1

Bundesdatenschutzgesetz (BDSG)

vom 20. Dezember 1990 (BGBl. I S. 2954), neugefasst durch Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Gesetz vom 29.07.2009 (BGBl. I, S. 2254), durch Artikel 5 des Gesetzes vom 29.07.2009 (BGBl. I, S. 2355 [2384] und durch Gesetz vom 14.08.2009 (BGBl. I, S. 2814)

Aktualisierte, nicht amtliche Fassung

Herausgeber: Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Stand: 11. Juni 2010

Hinweis: Im Hinblick auf die in § 47 enthaltene Übergangsregelung ist die alte Fassung des § 28 weiterhin in Kursivschrift wiedergegeben.

Inhaltsübersicht

Erster Abschnitt
Allgemeine und gemeinsame Bestimmungen

§ 1 Zweck und Anwendungsbereich des Gesetzes
§ 2 Öffentliche und nicht-öffentliche Stellen
§ 3 Weitere Begriffsbestimmungen
§ 3a Datenvermeidung und Datensparsamkeit
§ 4 Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung
§ 4a Einwilligung
§ 4b Übermittlung personenbezogener Daten ins Ausland sowie an über- und zwischenstaatliche Stellen
§ 4c Ausnahmen
§ 4d Meldepflicht
§ 4e Inhalt der Meldepflicht
§ 4f Beauftragter für den Datenschutz
§ 4g Aufgaben des Beauftragten für den Datenschutz
§ 5 Datengeheimnis
§ 6 Rechte des Betroffenen
§ 6a Automatisierte Einzelentscheidung
§ 6b Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen
§ 6c Mobile personenbezogene Speicher- und Verarbeitungsmedien
§ 7 Schadensersatz
§ 8 Schadensersatz bei automatisierter Datenverarbeitung durch öffentliche Stellen
§ 9 Technische und organisatorische Maßnahmen
§ 9a Datenschutzaudit
§ 10 Einrichtung automatisierter Abrufverfahren
§ 11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

Zweiter Abschnitt
Datenverarbeitung der öffentlichen Stellen

Erster Unterabschnitt
Rechtsgrundlagen der Datenverarbeitung

§ 12 Anwendungsbereich
§ 13 Datenerhebung
§ 14 Datenspeicherung, -veränderung und -nutzung
§ 15 Datenübermittlung an öffentliche Stellen
§ 16 Datenübermittlung an nicht-öffentliche Stellen
§ 17 weggefallen
§ 18 Durchführung des Datenschutzes in der Bundesverwaltung

Zweiter Unterabschnitt
Rechte des Betroffenen

§ 19 Auskunft an den Betroffenen
§ 19a Benachrichtigung
§ 20 Berichtigung, Löschung und Sperrung von Daten; Widerspruchsrecht
§ 21 Anrufung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Dritter Unterabschnitt
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit

§ 22 Wahl des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit
§ 23 Rechtsstellung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit
§ 24 Kontrolle durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit
§ 25 Beanstandungen durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

§ 26 Weitere Aufgaben des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Dritter Abschnitt
Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen

Erster Unterabschnitt
Rechtsgrundlagen der Datenverarbeitung

§ 27 Anwendungsbereich
§ 28 Datenerhebung und -speicherung für eigene Geschäftszwecke
§ 28a Datenübermittlung an Auskunfteien
§ 28b Scoring
§ 29 Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung
§ 30 Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung in anonymisierter Form
§ 30a Geschäftsmäßige Datenerhebung und -speicherung für Zwecke der Markt- oder Meinungsforschung
§ 31 Besondere Zweckbindung
§ 32 Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses

Zweiter Unterabschnitt
Rechte des Betroffenen

§ 33 Benachrichtigung des Betroffenen
§ 34 Auskunft an den Betroffenen
§ 35 Berichtigung, Löschung und Sperrung von Daten

Dritter Unterabschnitt
Aufsichtsbehörde

§ 36 weggefallen
§ 37 weggefallen
§ 38 Aufsichtsbehörde
§ 38a Verhaltensregeln zur Förderung der Durchführung datenschutzrechtlicher Regelungen

Vierter Abschnitt
Sondervorschriften

§ 39 Zweckbindung bei personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen
§ 40 Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen
§ 41 Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die Medien
§ 42 Datenschutzbeauftragter der Deutschen Welle
§ 42a Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

Fünfter Abschnitt
Schlussvorschriften

§ 43 Bußgeldvorschriften
§ 44 Strafvorschriften

Sechster Abschnitt
Übergangsvorschriften

§ 45 Laufende Verwendungen
§ 46 Weitergeltung von Begriffsbestimmungen
§ 47 Übergangsregelung
§ 48 Bericht der Bundesregierung

Anlage
(zu § 9 Satz 1)

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.

(11) Beschäftigte sind

1. Arbeitnehmerinnen und Arbeitnehmer,

2. zu ihrer Berufsbildung Beschäftigte,

3. Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden),

4. in anerkannten Werkstätten für behinderte Menschen Beschäftigte,

5. nach dem Jugendfreiwilligendienstegesetz Beschäftigte,

6. Personen, die wegen ihrer wirtschaftlichen Unselbstständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,

7. Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist,

8. Beamtinnen, Beamte, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende.

§ 3a
Datenvermeidung und Datensparsamkeit

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

§ 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 Einzel-

falles 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 30a 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 offensteht, 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 und die Informationsfreiheit 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 und die Informationsfreiheit nach Maßgabe von § 4e zu melden.

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

(3) Die Meldepflicht entfällt ferner, wenn die verantwortliche Stelle personenbezogene Daten für eigene Zwecke erhebt, verarbeitet oder nutzt, hierbei in der Regel höchstens neun Personen ständig mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt und entweder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit den Betroffenen erforderlich ist.

(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,

2. zum Zweck der anonymisierten Übermittlung oder

3. für Zwecke der Markt- oder Meinungsforschung

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 für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

(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 und die Informationsfreiheit 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 verarbeiten, 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 die nicht-öffentlichen Stellen, die in der Regel höchstens neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Soweit aufgrund der Struktur einer öffentlichen Stelle erforderlich, genügt die Bestellung eines Beauftragten für den Datenschutz für mehrere Bereiche. Soweit nicht-öffentliche Stellen automatisierte Verarbeitungen vornehmen, die einer Vorabkontrolle unterliegen, oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung automatisiert verarbeiten, haben sie unabhängig von der Anzahl der mit der automatisierten Verarbeitung beschäftigten Personen 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. Das Maß der erforderlichen Fachkunde bestimmt sich insbesondere nach dem Umfang der Datenverarbeitung der verantwortlichen Stelle und dem Schutzbedarf der personenbezogenen Daten, die die verantwortliche Stelle erhebt oder verwendet. Zum Beauftragten für den Datenschutz kann auch eine Person außerhalb der verantwortlichen Stelle bestellt werden; die Kontrolle erstreckt sich auch auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis nach § 30 der Abgabenordnung, unter-

liegen. 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. Ist nach Absatz 1 ein Beauftragter für den Datenschutz zu bestellen, so ist die Kündigung des Arbeitsverhältnisses unzulässig, es sei denn, dass Tatsachen vorliegen, welche die verantwortliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen. Nach der Abberufung als Beauftragter für den Datenschutz ist die Kündigung innerhalb eines Jahres nach der Beendigung der Bestellung unzulässig, es sei denn, dass die verantwortliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt ist. Zur Erhaltung der zur Erfüllung seiner Aufgaben erforderlichen Fachkunde hat die verantwortliche Stelle dem Beauftragten für den Datenschutz die Teilnahme an Fort- und Weiterbildungsveranstaltungen zu ermöglichen und deren Kosten zu übernehmen.

(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.

(4a) Soweit der Beauftragte für den Datenschutz bei seiner Tätigkeit Kenntnis von Daten erhält, für die dem Leiter oder einer bei der öffentlichen oder nicht-öffentlichen Stelle beschäftigten Person aus beruflichen Gründen ein Zeugnisverweigerungsrecht zusteht, steht dieses Recht auch dem Beauftragten für den Datenschutz und dessen Hilfspersonal zu. Über die Ausübung dieses Rechts entscheidet die Person, der das Zeugnisverweigerungsrecht aus beruflichen Gründen zusteht, es sei denn, dass diese Entscheidung in absehbarer Zeit nicht herbeigeführt werden kann. Soweit das Zeugnisverweigerungsrecht des Beauftragten für den Datenschutz reicht, unterliegen seine Akten und andere Schriftstücke einem Beschlagnahmeverbot.

(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 kann die Beratung nach § 38 Abs. 1 Satz 2 in Anspruch nehmen. 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. Der Beauftragte für den Datenschutz macht die Angaben nach § 4e Satz 1 Nr. 1 bis 8 auf Antrag jedermann in geeigneter Weise verfügbar.

(2a) Soweit bei einer nicht-öffentlichen Stelle keine Verpflichtung zur Bestellung eines Beauftragten für den Datenschutz besteht, hat der Leiter der nicht-öffentlichen Stelle die Erfüllung der Aufgaben nach den Absätzen 1 und 2 in anderer Weise sicherzustellen.

(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
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 und die Informationsfreiheit unterrichten. In diesem Fall richtet sich das weitere Verfahren nach § 19 Abs. 6.

(3) Personenbezogene Daten über die Ausübung eines Rechts des Betroffenen, das sich aus diesem Gesetz oder aus einer anderen Vorschrift über den Datenschutz ergibt, dürfen nur zur Erfüllung der sich aus der Ausübung des Rechts ergebenden Pflichten der verantwortlichen Stelle verwendet werden.

§ 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. Eine ausschließlich auf eine automatisierte Verarbeitung gestützte Entscheidung liegt insbesondere dann vor, wenn keine inhaltliche Bewertung und darauf gestützte Entscheidung durch eine natürliche Person stattgefunden hat.

(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 ist und die verantwortliche Stelle dem Betroffenen die Tatsache des Vorliegens einer Entscheidung im Sinne des Absatzes 1 mitteilt sowie auf Verlangen die wesentlichen Gründe dieser Entscheidung mitteilt und erläutert.

(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 Daten verarbeitende 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 und die Informationsfreiheit 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 insbesondere im Einzelnen festzulegen sind:

1. der Gegenstand und die Dauer des Auftrags,

2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,

3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,

4. die Berichtigung, Löschung und Sperrung von Daten,

5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,

6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,

7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,

8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,

9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,

10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Er kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden. Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.

(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 §§ 4 f, 4 g 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 Beschäftigungsverhältnisse erhoben, verarbeitet oder genutzt, gelten § 28

Abs. 2 Nummer 2 und die §§ 32 bis 35 anstelle der §§ 13 bis 16 und 19 bis 20.

§ 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 er-

heblich 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 Falle ist der Betroffene darauf hinzuweisen, dass er sich an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wenden kann.

(6) Wird dem Betroffenen keine Auskunft erteilt, so ist sie auf sein Verlangen dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit 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 und die Informationsfreiheit

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

§ 22
Wahl des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) Der Deutsche Bundestag wählt auf Vorschlag der Bundesregierung den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit 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 und die Informationsfreiheit

(1) Das Amtsverhältnis des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit 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 Bundes-

beauftragte 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 Falle 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 § 12 Abs. 6 sowie die §§ 13 bis 20 und 21a Abs. 5 des Bundesministergesetzes mit den Maßgaben anzuwenden, dass an die Stelle der vierjährigen 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. Abweichend von Satz 3 in Verbindung mit den §§ 15 bis 17 und 21 a Abs. 5 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.

(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 und die Informationsfreiheit

(1) der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit 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 Kon-

trolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind.

§ 25
Beanstandungen durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) Stellt der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit 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 und die Informationsfreiheit

(1) Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit 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 4 und 5 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 und -speicherung für eigene Geschäftszwecke

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

1. wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist,

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) Die Übermittlung oder Nutzung für einen anderen Zweck ist zulässig

1. unter den Voraussetzungen des Absatzes 1 Satz 1 Nummer 2 oder Nummer 3,

2. soweit es erforderlich ist

   a) zur Wahrung berechtigter Interessen eines Dritten oder

   b) zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten

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

3. 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.

(3) Die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke des Adresshandels oder der Werbung ist zulässig, soweit der Betroffene eingewilligt hat und im Falle einer nicht schriftlich erteilten Einwilligung die verantwortliche Stelle nach Absatz 3a verfährt. Darüber hinaus ist die Verarbeitung oder Nutzung personenbezogener Daten zulässig, soweit es sich um listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelt, die sich auf die Zugehörigkeit des Betroffenen zu dieser Personengruppe, seine Berufs-, Branchen- oder Geschäftsbezeichnung, seinen Namen, Titel, akademischen Grad, seine Anschrift und sein Geburtsjahr beschränken, und die Verarbeitung oder Nutzung erforderlich ist

1. für Zwecke der Werbung für eigene Angebote der verantwortlichen Stelle, die diese Daten mit Ausnahme der Angaben zur Gruppenzugehörigkeit beim Betroffenen nach Absatz 1 Satz 1 Nummer 1 oder aus allgemein zugänglichen Adress-, Rufnummern-, Branchen- oder vergleichbaren Verzeichnissen erhoben hat,

2. für Zwecke der Werbung im Hinblick auf die berufliche Tätigkeit des Betroffenen und unter seiner beruflichen Anschrift oder

3. für Zwecke der Werbung für Spenden, die nach § 10b Absatz 1 und § 34g des Einkommensteuergesetzes steuerbegünstigt sind.

Für Zwecke nach Satz 2 Nummer 1 darf die verantwortliche Stelle zu den dort genannten Daten weitere Daten hinzuspeichern. Zusammengefasste personenbezogene Daten nach Satz 2 dürfen auch dann für Zwecke der Werbung übermittelt werden, wenn die Übermittlung nach Maßgabe des § 34 Absatz 1a Satz 1 gespeichert

wird; in diesem Fall muss die Stelle, die die Daten erstmalig erhoben hat, aus der Werbung eindeutig hervorgehen. Unabhängig vom Vorliegen der Voraussetzungen des Satzes 2 dürfen personenbezogene Daten für Zwecke der Werbung für fremde Angebote genutzt werden, wenn für den Betroffenen bei der Ansprache zum Zwecke der Werbung die für die Nutzung der Daten verantwortliche Stelle eindeutig erkennbar ist. Eine Verarbeitung oder Nutzung nach den Sätzen 2 bis 4 ist nur zulässig, soweit schutzwürdige Interessen des Betroffenen nicht entgegenstehen. Nach den Sätzen 1, 2 und 4 übermittelte Daten dürfen nur für den Zweck verarbeitet oder genutzt werden, für den sie übermittelt worden sind.

(3a) Wird die Einwilligung nach § 4a Absatz 1 Satz 3 in anderer Form als der Schriftform erteilt, hat die verantwortliche Stelle dem Betroffenen den Inhalt der Einwilligung schriftlich zu bestätigen, es sei denn, dass die Einwilligung elektronisch erklärt wird und die verantwortliche Stelle sicherstellt, dass die Einwilligung protokolliert wird und der Betroffene deren Inhalt jederzeit abrufen und die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie in drucktechnisch deutlicher Gestaltung besonders hervorzuheben.

(3b) Die verantwortliche Stelle darf den Abschluss eines Vertrags nicht von einer Einwilligung des Betroffenen nach Absatz 3 Satz 1 abhängig machen, wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist. Eine unter solchen Umständen erteilte Einwilligung ist unwirksam.

(4) Widerspricht der Betroffene bei der verantwortlichen Stelle der Verarbeitung oder Nutzung seiner Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung, ist eine Verarbeitung oder Nutzung für diese Zwecke unzulässig. Der Betroffene ist bei der Ansprache zum Zweck der Werbung oder der Markt- oder Meinungsforschung und in den Fällen des Absatzes 1 Satz 1 Nummer 1 auch bei Begründung des rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses 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 im Rahmen der Zwecke nach Absatz 3 übermittelt worden sind, der Verarbeitung oder Nutzung zum Zwecke der Werbung oder der Markt- oder Meinungsforschung, hat dieser die Daten für diese Zwecke zu sperren. In den Fällen des Absatzes 1 Satz 1 Nummer 1 darf für den Widerspruch keine strengere Form verlangt werden als für die Begründung des rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses.

(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 2 Nummer 2 Buchstabe b gilt entsprechend.

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

(bis zum 31.08.2009 geltende Fassung, vgl. Übergangsregelung in § 47)

(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 zum 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.

§ 28a
Datenübermittlung an Auskunfteien

(1) Die Übermittlung personenbezogener Daten über eine Forderung an Auskunfteien ist nur zulässig, soweit die geschuldete Leistung trotz Fälligkeit nicht erbracht worden ist, die Übermittlung zur Wahrung berechtigter Interessen der verantwortlichen Stelle oder eines Dritten erforderlich ist und

1. die Forderung durch ein rechtskräftiges oder für vorläufig vollstreckbar erklärtes Urteil festgestellt worden ist oder ein Schuldtitel nach § 794 der Zivilprozessordnung vorliegt,

2. die Forderung nach § 178 der Insolvenzordnung festgestellt und nicht vom Schuldner im Prüfungstermin bestritten worden ist,

3. der Betroffene die Forderung ausdrücklich anerkannt hat,

4. a) der Betroffene nach Eintritt der Fälligkeit der Forderung mindestens zweimal schriftlich gemahnt worden ist,

   b) zwischen der ersten Mahnung und der Übermittlung mindestens vier Wochen liegen,

   c) die verantwortliche Stelle den Betroffenen rechtzeitig vor der Übermittlung der Angaben, jedoch frühestens bei der ersten Mahnung über die bevorstehende Übermittlung unterrichtet hat und

   d) der Betroffene die Forderung nicht bestritten hat oder

5. das der Forderung zugrunde liegende Vertragsverhältnis aufgrund von Zahlungsrückständen fristlos gekündigt werden kann und die verantwortliche Stelle den Betroffenen über die bevorstehende Übermittlung unterrichtet hat.

Satz 1 gilt entsprechend, wenn die verantwortliche Stelle selbst die Daten nach § 29 verwendet.

2) Zur zukünftigen Übermittlung nach § 29 Abs. 2 dürfen Kreditinstitute personenbezogene Daten über die Begründung, ordnungsgemäße Durchführung und Beendigung eines Vertragsverhältnisses betreffend ein Bankgeschäft nach § 1 Abs. 1 Satz 2 Nr. 2, 8 oder Nr. 9 des Kre-

ditwesengesetzes an Auskunfteien übermitteln, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Übermittlung gegenüber dem Interesse der Auskunftei an der Kenntnis der Daten offensichtlich überwiegt. Der Betroffene ist vor Abschluss des Vertrages hierüber zu unterrichten. Satz 1 gilt nicht für Giroverträge, die die Einrichtung eines Kontos ohne Überziehungsmöglichkeit zum Gegenstand haben. Zur zukünftigen Übermittlung nach § 29 Abs. 2 ist die Übermittlung von Daten über Verhaltensweisen des Betroffenen, die im Rahmen eines vorvertraglichen Vertrauensverhältnisses der Herstellung von Markttransparenz dienen, an Auskunfteien auch mit Einwilligung des Betroffenen unzulässig.

(3) Nachträgliche Änderungen der einer Übermittlung nach Absatz 1 oder Absatz 2 zugrunde liegenden Tatsachen hat die verantwortliche Stelle der Auskunftei innerhalb von einem Monat nach Kenntniserlangung mitzuteilen, solange die ursprünglich übermittelten Daten bei der Auskunftei gespeichert sind. Die Auskunftei hat die übermittelnde Stelle über die Löschung der ursprünglich übermittelten Daten zu unterrichten.

§ 28b
Scoring

(1) Zum Zwecke der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dem Betroffenen darf ein Wahrscheinlichkeitswert für ein bestimmtes zukünftiges Verhalten des Betroffenen erhoben oder verwendet werden, wenn

1. die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sind,

2. im Falle der Berechnung des Wahrscheinlichkeitswerts durch eine Auskunftei die Voraussetzungen für eine Übermittlung der genutzten Daten nach § 29 und in allen anderen Fällen die Voraussetzungen einer zulässigen Nutzung der Daten nach § 28 vorliegen,

3. für die Berechnung des Wahrscheinlichkeitswerts nicht ausschließlich Anschriftendaten genutzt werden,

4. im Falle der Nutzung von Anschriftendaten der Betroffene vor Berechnung des Wahrscheinlichkeitswerts über die vorgesehene Nutzung dieser Daten unterrichtet worden ist; die Unterrichtung ist zu dokumentieren.

§ 29
Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung

(1) Das geschäftsmäßige Erheben, Speichern, Verändern oder Nutzen personenbezogener Daten zum Zweck der Übermittlung, insbesondere wenn dies der Werbung, der Tätigkeit von Auskunfteien oder dem Adresshandel 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,

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, Speiche-

rung oder Veränderung offensichtlich überwiegt, oder

3. die Voraussetzungen des § 28a Abs. 1 oder Abs. 2 erfüllt sind; Daten im Sinne von § 28a Abs. 2 Satz 4 dürfen nicht erhoben oder gespeichert werden.

§ 28 Absatz 1 Satz 2 und Absatz 3 bis 3b ist anzuwenden.

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

1. der Dritte, dem die Daten übermittelt werden, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat und

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

§ 28 Absatz 3 bis 3b gilt entsprechend. Bei der Übermittlung nach Satz 1 Nr. 1 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. Die übermittelnde Stelle hat Stichprobenverfahren nach § 10 Abs. 4 Satz 3 durchzuführen und dabei auch das Vorliegen eines berechtigten Interesses einzelfallbezogen festzustellen und zu überprüfen.

(3) Die Aufnahme personenbezogener Daten in elektronische oder gedruckte Adress-, Rufnummern-, 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.

(6) Eine Stelle, die geschäftsmäßig personenbezogene Daten, die zur Bewertung der Kreditwürdigkeit von Verbrauchern genutzt werden dürfen, zum Zweck der Übermittlung erhebt, speichert oder verändert, hat Auskunftsverlangen von Darlehensgebern aus anderen Mitgliedstaaten der Europäischen Union oder anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum genauso zu behandeln wie Auskunftsverlangen inländischer Darlehensgeber.

(7) Wer den Abschluss eines Verbraucherdarlehensvertrags oder eines Vertrags über eine entgeltliche Finanzierungshilfe mit einem Verbraucher infolge einer Auskunft einer Stelle im Sinne des Absatzes 6 ablehnt, hat den Verbraucher unverzüglich hierüber sowie über die erhaltene Auskunft zu unterrichten. Die Unterrichtung unterbleibt, soweit hierdurch die öffentliche Sicherheit oder Ordnung gefährdet würde. § 6a bleibt unberührt.

§ 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.

§ 30a
Geschäftsmäßige Datenerhebung und -speicherung für Zwecke der Markt- oder Meinungsforschung

(1) Das geschäftsmäßige Erheben, Verarbeiten oder Nutzen personenbezogener Daten für Zwecke der Markt- oder Meinungsforschung ist zulässig, wenn

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

2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte und das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung gegenüber dem Interesse der verantwortlichen Stelle nicht offensichtlich überwiegt.

Besondere Arten personenbezogener Daten (§ 3 Absatz 9) dürfen nur für ein bestimmtes Forschungsvorhaben erhoben, verarbeitet oder genutzt werden.

(2) Für Zwecke der Markt- oder Meinungsforschung erhobene oder gespeicherte personenbezogene Daten dürfen nur für diese Zwecke verarbeitet oder genutzt werden. Daten, die nicht aus allgemein zugänglichen Quellen entnommen worden sind und die die verantwortliche Stelle auch nicht veröffentlichen darf, dürfen nur für das Forschungsvorhaben verarbeitet oder genutzt werden, für das sie erhoben worden sind. Für einen anderen Zweck dürfen sie nur verarbeitet oder genutzt werden, wenn sie zuvor so anonymisiert werden, dass ein Personenbezug nicht mehr hergestellt werden kann.

(3) Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Zweck des Forschungsvorhabens, für das die Daten erhoben worden sind, 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. Diese Merkmale dürfen mit den Einzelangaben nur zusammengeführt werden, soweit dies nach dem Zweck des Forschungsvorhabens erforderlich ist.

(4) § 29 gilt nicht.

(5) § 28 Absatz 4 und 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
Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses

(1) Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

(2) Absatz 1 ist auch anzuwenden, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ohne dass sie automatisiert verarbeitet oder in oder aus einer nicht automatisierten Datei verarbeitet, genutzt oder für die Verarbeitung oder Nutzung in einer solchen Datei erhoben werden.

(3) Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt.

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,

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 Absatz 2 Satz 2)

   und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist,

9. aus allgemein zugänglichen Quellen entnommene Daten geschäftsmäßig für Zwecke der Markt- oder Meinungsforschung gespeichert sind 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) Die verantwortliche Stelle hat dem Betroffenen auf Verlangen Auskunft zu erteilen über

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

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

3. den Zweck der Speicherung.

Der Betroffene soll die Art der personenbezogenen Daten, über die

Auskunft erteilt werden soll, näher bezeichnen. Werden die personenbezogenen Daten geschäftsmäßig zum Zweck der Übermittlung gespeichert, ist Auskunft über die Herkunft und die Empfänger auch dann zu erteilen, wenn diese Angaben nicht gespeichert sind. Die Auskunft über die Herkunft und die Empfänger kann verweigert werden, soweit das Interesse an der Wahrung des Geschäftsgeheimnisses gegenüber dem Informationsinteresse des Betroffenen überwiegt.

(1a) Im Fall des § 28 Abs. 3 Satz 4 hat die übermittelnde Stelle die Herkunft der Daten und den Empfänger für die Dauer von zwei Jahren nach der Übermittlung zu speichern und dem Betroffenen auf Verlangen Auskunft über die Herkunft der Daten und den Empfänger zu erteilen. Satz 1 gilt entsprechend für den Empfänger.

(2) Im Fall des § 28b hat die für die Entscheidung verantwortliche Stelle dem Betroffenen auf Verlangen Auskunft zu erteilen über

1. die innerhalb der letzten sechs Monate vor dem Zugang des Auskunftsverlangens erhobenen oder erstmalig gespeicherten Wahrscheinlichkeitswerte,

2. die zur Berechnung der Wahrscheinlichkeitswerte genutzten Datenarten und

3. das Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte einzelfallbezogen und nachvollziehbar in allgemein verständlicher Form.

Satz 1 gilt entsprechend, wenn die für die Entscheidung verantwortliche Stelle

1. die zur Berechnung der Wahrscheinlichkeitswerte genutzten Daten ohne Personenbezug speichert, den Personenbezug aber bei der Berechnung herstellt oder

2. bei einer anderen Stelle gespeicherte Daten nutzt.

Hat eine andere als die für die Entscheidung verantwortliche Stelle

1. den Wahrscheinlichkeitswert oder

2. einen Bestandteil des Wahrscheinlichkeitswerts

berechnet, hat sie die insoweit zur Erfüllung der Auskunftsansprüche nach den Sätzen 1 und 2 erforderlichen Angaben auf Verlangen der für die Entscheidung verantwortlichen Stelle an diese zu übermitteln. Im Falle des Satzes 3 Nr. 1 hat die für die Entscheidung verantwortliche Stelle den Betroffenen zur Geltendmachung seiner Auskunftsansprüche unter Angabe des Namens und der Anschrift der anderen Stelle sowie der zur Bezeichnung des Einzelfalls notwendigen Angaben unverzüglich an diese zu verweisen, soweit sie die Auskunft nicht selbst erteilt. In diesem Fall hat die andere Stelle, die den Wahrscheinlichkeitswert berechnet hat, die Auskunftsansprüche nach den Sätzen 1 und 2 gegenüber dem Betroffenen unentgeltlich zu erfüllen. Die Pflicht der für die Berechnung des Wahrscheinlichkeitswerts verantwortlichen Stelle nach Satz 3 entfällt, soweit die für die Entscheidung verantwortliche Stelle von ihrem Recht nach Satz 4 Gebrauch macht.

(3) Eine Stelle, die geschäftsmäßig personenbezogene Daten zum Zwecke der Übermittlung speichert, hat dem Betroffenen auf Verlangen Auskunft über die zu seiner Person gespeicherten Daten zu erteilen, auch wenn sie weder automa-

tisiert verarbeitet werden noch in einer nicht automatisierten Datei gespeichert sind. Dem Betroffenen ist auch Auskunft zu erteilen über Daten, die

1. gegenwärtig noch keinen Personenbezug aufweisen, bei denen ein solcher aber im Zusammenhang mit der Auskunftserteilung von der verantwortlichen Stelle hergestellt werden soll,

2. die verantwortliche Stelle nicht speichert, aber zum Zweck der Auskunftserteilung nutzt.

Die Auskunft über die Herkunft und die Empfänger kann verweigert werden, soweit das Interesse an der Wahrung des Geschäftsgeheimnisses gegenüber dem Informationsinteresse des Betroffenen überwiegt.

(4) Eine Stelle, die geschäftsmäßig personenbezogene Daten zum Zweck der Übermittlung erhebt, speichert oder verändert, hat dem Betroffenen auf Verlangen Auskunft zu erteilen über

1. die innerhalb der letzten zwölf Monate vor dem Zugang des Auskunftsverlangens übermittelten Wahrscheinlichkeitswerte für ein bestimmtes zukünftiges Verhalten des Betroffenen sowie die Namen und letztbekannten Anschriften der Dritten, an die die Werte übermittelt worden sind,

2. die Wahrscheinlichkeitswerte, die sich zum Zeitpunkt des Auskunftsverlangens nach den von der Stelle zur Berechnung angewandten Verfahren ergeben,

3. die zur Berechnung der Wahrscheinlichkeitswerte nach den Nummern 1 und 2 genutzten Datenarten sowie

4. das Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte einzelfallbezogen und nachvollziehbar in allgemein verständlicher Form.

Satz 1 gilt entsprechend, wenn die verantwortliche Stelle

1. die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten ohne Personenbezug speichert, den Personenbezug aber bei der Berechnung herstellt oder

2. bei einer anderen Stelle gespeicherte Daten nutzt.

(5) Die nach den Absätzen 1a bis 4 zum Zweck der Auskunftserteilung an den Betroffenen gespeicherten Daten dürfen nur für diesen Zweck sowie für Zwecke der Datenschutzkontrolle verwendet werden; für andere Zwecke sind sie zu sperren.

(6) Die Auskunft ist auf Verlangen in Textform zu erteilen, soweit nicht wegen der besonderen Umstände eine andere Form der Auskunftserteilung angemessen ist.

(7) 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.

(8) Die Auskunft ist unentgeltlich. Werden die personenbezogenen Daten geschäftsmäßig zum Zweck der Übermittlung gespeichert, kann der Betroffene einmal je Kalenderjahr eine unentgeltliche Auskunft in Textform verlangen. Für jede weitere Auskunft kann ein Entgelt verlangt werden, wenn der Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen kann. Das Entgelt darf über die durch die Auskunfts-

erteilung entstandenen unmittelbar zurechenbaren Kosten nicht hinausgehen. Ein Entgelt kann nicht verlangt werden, wenn

1. besondere Umstände die Annahme rechtfertigen, dass Daten unrichtig oder unzulässig gespeichert werden, oder

2. die Auskunft ergibt, dass die Daten nach § 35 Abs. 1 zu berichtigen oder unter nach § 35 Abs. 2 Satz 2 Nr. 1 zu löschen sind.

(9) 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 hinzuweisen.

§ 35
Berichtigung, Löschung und Sperrung von Daten

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Geschätzte Daten sind als solche deutlich zu kennzeichnen.

(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, Gewerkschaftszugehörigkeit, Gesundheit, 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, soweit es sich um Daten über erledigte Sachverhalte handelt und der Betroffene der Löschung nicht widerspricht, am Ende des dritten Kalenderjahres beginnend mit dem Kalenderjahr, das der erstmaligen Speicherung folgt, ergibt, dass eine längerwährende Speicherung nicht erforderlich ist.

Personenbezogene Daten, die auf der Grundlage von § 28a Abs. 2 Satz 1 oder § 29 Abs. 1 Satz 1 Nr. 3 gespeichert werden, sind nach Beendigung des Vertrages auch zu löschen, wenn der Betroffene dies verlangt.

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

1. im Fall des Absatzes 2 Satz 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.

(4a) Die Tatsache der Sperrung darf nicht übermittelt werden.

(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 wurden, 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
(weggefallen)

§ 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. Sie berät und unterstützt die Beauftragten für den Datenschutz und die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse. 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 der Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz kann die Aufsichtsbehörde Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel anordnen. Bei schwerwiegenden Verstößen oder Mängeln, insbesondere solchen, die mit einer besonderen Gefährdung des Persönlichkeitsrechts verbunden sind, kann sie die Erhebung, Verarbeitung oder Nutzung oder den Einsatz einzelner Verfahren untersagen, wenn die Verstöße oder 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 und die Informationsfreiheit 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 und die Informationsfreiheit.

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

§ 42a
Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

Stellt eine nicht-öffentliche Stelle im Sinne des § 2 Abs. 4 oder eine öffentliche Stelle nach § 27 Abs. 1 Satz 1 Nr. 2 fest, dass bei ihr gespeicherte

1. besondere Arten personenbezogener Daten (§ 3 Abs. 9),

2. personenbezogene Daten, die einem Berufsgeheimnis unterliegen,

3. personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen oder

4. personenbezogene Daten zu Bank- oder Kreditkartenkonten

unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, hat sie dies nach den Sätzen 2 bis 5 unverzüglich der zuständigen Aufsichtsbehörde sowie den Betroffenen mitzuteilen. Die Benachrichtigung des Betroffenen muss unverzüglich erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden oder nicht unverzüglich erfolgt sind und die Strafverfolgung nicht mehr gefährdet wird. Die Benachrichtigung der Betroffenen muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung und Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten. Die Benachrichtigung der zuständigen Aufsichtsbehörde muss zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung und der von der Stelle daraufhin ergriffenen Maßnahmen enthalten. Soweit die Benachrichtigung der Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, insbesondere aufgrund der Vielzahl der betroffenen Fälle, tritt an ihre Stelle die Information der Öffentlichkeit durch Anzeigen, die mindestens eine halbe Seite umfassen, in mindestens zwei bundesweit erscheinenden Tageszeitungen oder durch eine andere, in ihrer Wirksamkeit hinsichtlich der Information der Betroffenen gleich geeignete Maßnahme. Eine Benachrichtigung, die der Benachrichtigungspflichtige erteilt hat, darf in einem Strafverfahren oder in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen ihn oder einen in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen des Benachrichtigungspflichtigen nur mit Zustimmung des Benachrichtigungspflichtigen verwendet werden.

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,

2a. entgegen § 10 Abs. 4 Satz 3 nicht gewährleistet, dass die Datenübermittlung festgestellt und überprüft werden kann,

2b. entgegen § 11 Abs. 2 Satz 2 einen Auftrag nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt oder entgegen § 11 Abs. 2 Satz 4 sich nicht vor Beginn der Datenverarbeitung über die Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt,

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,

3a. entgegen § 28 Abs. 4 Satz 4 eine strengere Form verlangt,

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

4a. entgegen § 28a Abs. 3 Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,

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,

7a. entgegen § 29 Abs. 6 ein Auskunftsverlangen nicht richtig behandelt,

7b. entgegen § 29 Abs. 7 Satz 1 einen Verbraucher nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet,

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

8a. entgegen § 34 Abs. 1 Satz 1, auch in Verbindung mit Satz 3, entgegen § 34 Abs. 1a, entgegen § 34 Abs. 2 Satz 1, auch in Verbindung mit Satz 2, oder entgegen § 34 Abs. 2 Satz 5, Abs. 3 Satz 1 oder Satz 2 oder Abs. 4 Satz 1, auch in Verbindung mit Satz 2, eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder entgegen § 34 Abs. 1a Daten nicht speichert,

8b. entgegen § 34 Abs. 2 Satz 3 Angaben nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt,

8c. entgegen § 34 Abs. 2 Satz 4 den Betroffenen nicht oder nicht rechtzeitig an die andere Stelle verweist,

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,

5a. entgegen § 28 Abs. 3b den Abschluss eines Vertrages von der Einwilligung des Betroffenen abhängig macht,

5b. entgegen § 28 Abs. 4 Satz 1 Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung verarbeitet oder nutzt,

6. entgegen § 30 Abs. 1 Satz 2, § 30a Abs. 3 Satz 3 oder § 40 Abs. 2 Satz 3 ein dort genanntes Merkmal mit einer Einzelangabe zusammenführt oder

7. entgegen § 42a Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht.

(3) Die Ordnungswidrigkeit kann im Fall des Absatzes 1 mit einer Geldbuße bis zu fünfzigtausend Euro, in den Fällen des Absatzes 2 mit einer Geldbuße bis zu dreihunderttausend Euro geahndet werden. Die Geldbuße soll den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen. Reichen die in Satz 1 genannten Beträge hierfür nicht aus, so können sie überschritten 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 Informationsfreiheit 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.

§ 47
Übergangsregelung

Für die Verarbeitung und Nutzung vor dem 1. September 2009 erhobener oder gespeicherter Daten ist § 28 in der bis dahin geltenden Fassung weiter anzuwenden

1. für Zwecke der Markt- oder Meinungsforschung bis zum 31. August 2010,

2. für Zwecke der Werbung bis zum 31. August 2012.

§ 48
Bericht der Bundesregierung

Die Bundesregierung berichtet dem Bundestag

1. bis zum 31. Dezember 2012 über die Auswirkungen der §§ 30a und 42a,

2. bis zum 31. Dezember 2014 über die Auswirkungen der Änderungen der §§ 28 und 29.

Sofern sich aus Sicht der Bundesregierung gesetzgeberische Maßnahmen empfehlen, soll der Bericht einen Vorschlag enthalten.

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.

Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

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

Erwägungsgründe

KAPITEL I – ALLGEMEINE BESTIMMUNGEN
Artikel 1 – Gegenstand der Richtlinie
Artikel 2 – Begriffsbestimmungen
Artikel 3 – Anwendungsbereich
Artikel 4 – Anwendbares einzelstaatliches Recht

KAPITEL II – ALLGEMEINE BEDINGUNGEN FÜR DIE RECHTMÄSSIGKEIT DER VERARBEITUNG PERSONENBEZOGENER DATEN
Artikel 5

Abschnitt I – Grundsätze in Bezug auf die Qualität
Artikel 6

Abschnitt II – Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung von Daten
Artikel 7

Abschnitt III – Besondere Kategorien der Verarbeitung
Artikel 8 – Verarbeitung besonderer Kategorien personenbezogener Daten
Artikel 9 – Verarbeitung personenbezogener Daten und Meinungsfreiheit

Abschnitt IV – Information der betroffenen Person
Artikel 10 – Information bei der Erhebung personenbezogener Daten bei der betroffenen Person
Artikel 11 – Informationen für den Fall, dass die Daten nicht bei der betroffenen Person erhoben wurden

Abschnitt V – Auskunftsrecht der betroffenen Person
Artikel 12 – Auskunftsrecht

Abschnitt VI – Ausnahmen und Einschränkungen
Artikel 13 – Ausnahmen und Einschränkungen

Abschnitt VII – Widerspruchsrecht der betroffenen Person
Artikel 14 – Widerspruchsrecht der betroffenen Person
Artikel 15 – Automatisierte Einzelentscheidungen

Abschnitt VIII – Vertraulichkeit und Sicherheit
Artikel 16 – Vertraulichkeit der Verarbeitung
Artikel 17 – Sicherheit der Verarbeitung

Abschnitt IX – Meldung
Artikel 18 – Pflicht zur Meldung bei der Kontrollstelle
Artikel 19 – Inhalt der Meldung
Artikel 20 – Vorabkontrolle
Artikel 21 – Öffentlichkeit der Verarbeitungen

KAPITEL III – RECHTSBEHELFE, HAFTUNG UND SANKTIONEN
Artikel 22 – Rechtsbehelfe
Artikel 23 – Haftung
Artikel 24 – Sanktionen

KAPITEL IV – ÜBERMITTLUNG PERSONENBEZOGENER DATEN IN DRITTLÄNDER
Artikel 25 – Grundsätze
Artikel 26 – Ausnahmen

KAPITEL V – VERHALTENSREGELN
Artikel 27

KAPITEL VI – KONTROLLSTELLE UND GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN
Artikel 28 – Kontrollstelle
Artikel 29 – Datenschutzgruppe
Artikel 30

KAPITEL VII – GEMEINSCHAFTLICHE DURCHFÜHRUNGSMASSNAHMEN
Artikel 31 – Ausschussverfahren

SCHLUSSBESTIMMUNGEN
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 Landesverteidi-

gung, 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 Rechte 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 an-

deren 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 dem 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 unver-

einbar 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 erhalten, 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 offensteht.

(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 Kon-

trollstellen 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 Kennnummer 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 geografischen 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 neuesten 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 Berufsgeheimnis 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 offensteht.

(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 Infor-

mation der Öffentlichkeit bestimmt sind und die entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offenstehen.

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 offensteht, 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 Ermahnung 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 vor-

sehen, 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 Entscheidungen (BVerfGE 27, 1 [6] – Mikrozensus; 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 Verfassungswegen 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

Auszug aus dem Urteil des Ersten Senats des Bundesverfassungsgerichts vom 27. Februar 2008 – 1 BvR 370/07, 1 BvR 595/07 –

Leitsätze der Entscheidung:

1. Das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) umfasst das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

2. Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Die Maßnahme kann schon dann gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für das überragend wichtige Rechtsgut hinweisen.

3. Die heimliche Infiltration eines informationstechnischen Systems ist grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen. Das Gesetz, das zu einem solchen Eingriff ermächtigt, muss Vorkehrungen enthalten, um den Kernbereich privater Lebensgestaltung zu schützen.

4. Soweit eine Ermächtigung sich auf eine staatliche Maßnahme beschränkt, durch welche die Inhalte und Umstände der laufenden Telekommunikation im Rechnernetz erhoben oder darauf bezogene Daten ausgewertet werden, ist der Eingriff an Art. 10 Abs. 1 GG zu messen.

5. Verschafft der Staat sich Kenntnis von Inhalten der Internetkommunikation auf dem dafür technisch vorgesehenen Weg, so liegt darin nur dann ein Eingriff in Art. 10 Abs. 1 GG, wenn die staatliche Stelle nicht durch Kommunikationsbeteiligte zur Kenntnisnahme autorisiert ist. Nimmt der Staat im Internet öffentlich zugängliche Kommunikationsinhalte wahr oder beteiligt er sich an öffentlich zugänglichen Kommunikationsvorgängen, greift er grundsätzlich nicht in Grundrechte ein.

Auszug aus Abschnitt C. des Urteils:

§ 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG, der den heimlichen Zugriff auf informationstechnische Systeme regelt, verletzt das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) in seiner besonderen Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

...

1. § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG ermächtigt zu Eingriffen in das allgemeine Persönlichkeitsrecht in seiner besonderen Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme; sie tritt zu den anderen Konkretisierungen dieses Grundrechts, wie dem Recht auf informationelle Selbstbestimmung, sowie zu den Freiheitsgewährleistungen der Art. 10 und Art. 13 GG hinzu, soweit diese keinen oder keinen hinreichenden Schutz gewähren.

a) Das allgemeine Persönlichkeitsrecht gewährleistet Elemente der Persönlichkeit, die nicht Gegenstand der besonderen Freiheitsgarantien des Grundgesetzes sind, diesen aber in ihrer konstituierenden Bedeutung für die Persönlichkeit nicht nachstehen (vgl. BVerfGE 99, 185 <193>; 114, 339 <346>). Einer solchen lückenschließenden Gewährleistung bedarf es insbesondere, um neuartigen Gefährdungen zu begegnen, zu denen es im Zuge des wissenschaftlich-technischen Fortschritts und gewandelter Lebensverhältnisse kommen kann (vgl. BVerfGE 54, 148 <153>; 65, 1 <41> ; BVerfG, Beschluss vom 13. Juni 2007 – 1 BvR 1550/03 u.a. –, NJW 2007, S. 2464 <2465>). Die Zuordnung eines konkreten Rechtsschutzbegehrens zu den verschiedenen Aspekten des Persönlichkeitsrechts richtet sich vor allem nach der Art der Persönlichkeitsgefährdung (vgl. BVerfGE 101, 361 <380>; 106, 28 <39>).

b) Die Nutzung der Informationstechnik hat für die Persönlichkeit und die Entfaltung des Einzelnen eine früher nicht absehbare Bedeutung erlangt. Die moderne Informationstechnik eröffnet dem Einzelnen neue Möglichkeiten, begründet aber auch neuartige Gefährdungen der Persönlichkeit.

aa) Die jüngere Entwicklung der Informationstechnik hat dazu geführt, dass informationstechnische Systeme allgegenwärtig sind und ihre Nutzung für die Lebensführung vieler Bürger von zentraler Bedeutung ist.

Dies gilt zunächst für Personalcomputer, über die mittlerweile eine deutliche Mehrheit der Haushalte in der Bundesrepublik verfügt (vgl. Statistisches Bundesamt, Statistisches Jahrbuch 2007, S. 113). Die Leistungs-

fähigkeit derartiger Rechner ist ebenso gestiegen wie die Kapazität ihrer Arbeitsspeicher und der mit ihnen verbundenen Speichermedien. Heutige Personalcomputer können für eine Vielzahl unterschiedlicher Zwecke genutzt werden, etwa zur umfassenden Verwaltung und Archivierung der eigenen persönlichen und geschäftlichen Angelegenheiten, als digitale Bibliothek oder in vielfältiger Form als Unterhaltungsgerät. Dementsprechend ist die Bedeutung von Personalcomputern für die Persönlichkeitsentfaltung erheblich gestiegen.

Die Relevanz der Informationstechnik für die Lebensgestaltung des Einzelnen erschöpft sich nicht in der größeren Verbreitung und Leistungsfähigkeit von Personalcomputern. Daneben enthalten zahlreiche Gegenstände, mit denen große Teile der Bevölkerung alltäglich umgehen, informationstechnische Komponenten. So liegt es beispielsweise zunehmend bei Telekommunikationsgeräten oder elektronischen Geräten, die in Wohnungen oder Kraftfahrzeugen enthalten sind.

bb) Der Leistungsumfang informationstechnischer Systeme und ihre Bedeutung für die Persönlichkeitsentfaltung nehmen noch zu, wenn solche Systeme miteinander vernetzt werden. Dies wird insbesondere aufgrund der gestiegenen Nutzung des Internet durch große Kreise der Bevölkerung mehr und mehr zum Normalfall.

Eine Vernetzung informationstechnischer Systeme ermöglicht allgemein, Aufgaben auf diese Systeme zu verteilen und insgesamt die Rechenleistung zu erhöhen. So können etwa die von einzelnen der vernetzten Systeme gelieferten Daten ausgewertet und die Systeme zu bestimmten Reaktionen veranlasst werden. Auf diese Weise kann zugleich der Funktionsumfang des einzelnen Systems erweitert werden.

Insbesondere das Internet als komplexer Verbund von Rechnernetzen öffnet dem Nutzer eines angeschlossenen Rechners nicht nur den Zugriff auf eine praktisch unübersehbare Fülle von Informationen, die von anderen Netzrechnern zum Abruf bereitgehalten werden. Es stellt ihm daneben zahlreiche neuartige Kommunikationsdienste zur Verfügung, mit deren Hilfe er aktiv soziale Verbindungen aufbauen und pflegen kann. Zudem führen technische Konvergenzeffekte dazu, dass auch herkömmliche Formen der Fernkommunikation in weitem Umfang auf das Internet verlagert werden können (vgl. etwa zur Sprachtelefonie Katko, CR 2005, S. 189).

cc) Die zunehmende Verbreitung vernetzter informationstechnischer Systeme begründet für den Einzelnen neben neuen Möglichkeiten der Persönlichkeitsentfaltung auch neue Persönlichkeitsgefährdungen.

(1) Solche Gefährdungen ergeben sich bereits daraus, dass komplexe informationstechnische Systeme wie etwa Personalcomputer ein breites Spektrum von Nutzungsmöglichkeiten eröffnen, die sämtlich mit der Erzeugung, Verarbeitung und Speicherung von Daten verbunden sind. Dabei handelt es sich nicht nur um Daten, die der Nutzer des Rechners bewusst anlegt oder speichert. Im Rahmen des Datenverarbeitungsprozesses erzeugen informationstechnische Systeme zudem selbsttätig zahlreiche weitere Daten, die ebenso wie die vom Nutzer gespeicherten Daten im Hinblick auf sein Verhalten und seine Eigenschaften ausgewertet werden können. In der Folge können sich im Arbeitsspeicher und auf den Speichermedien solcher Systeme eine Vielzahl von Daten mit Bezug zu den persönlichen Verhältnissen, den sozialen Kontakten und den ausgeübten Tätigkeiten des Nutzers finden. Werden diese Daten von Dritten erhoben und ausgewertet, so kann dies weitreichende Rückschlüsse auf die Persönlichkeit des Nutzers bis hin zu einer Profilbildung ermöglichen (vgl. zu den aus solchen Folgerungen entstehenden Persönlichkeitsgefährdungen BVerfGE 65, 1 <42>).

(2) Bei einem vernetzten, insbesondere einem an das Internet angeschlossenen System werden diese Gefährdungen in verschiedener Hinsicht vertieft. Zum einen führt die mit der Vernetzung verbundene Erweiterung der Nutzungsmöglichkeiten dazu, dass gegenüber einem alleinstehenden System eine noch größere Vielzahl und Vielfalt von Daten erzeugt, verarbeitet und gespeichert werden. Dabei handelt es sich um Kommunikationsinhalte sowie um Daten mit Bezug zu der Netzkommunikation. Durch die Speicherung und Auswertung solcher Daten über das Verhalten der Nutzer im Netz können weitgehende Kenntnisse über die Persönlichkeit des Nutzers gewonnen werden.

Vor allem aber öffnet die Vernetzung des Systems Dritten eine technische Zugriffsmöglichkeit, die genutzt werden kann, um die auf dem System vorhandenen Daten auszuspähen oder zu manipulieren. Der Einzelne kann solche Zugriffe zum Teil gar nicht wahrnehmen, jedenfalls aber nur begrenzt abwehren. Informationstechnische Systeme haben mittlerweile einen derart hohen Komplexitätsgrad erreicht, dass ein wirkungsvoller sozialer oder technischer Selbstschutz erhebliche Schwierigkeiten aufwerfen und zumindest den durchschnittlichen Nutzer überfordern kann. Ein technischer Selbstschutz kann zudem mit einem hohen Aufwand oder mit Funktionseinbußen des geschützten Systems verbunden sein. Viele Selbstschutzmöglichkeiten – etwa die Verschlüsselung oder die Verschleierung sensibler Daten – werden überdies weitgehend wirkungslos, wenn Dritten die Infiltration des Systems, auf dem die Daten abgelegt worden sind, einmal gelungen ist. Schließlich kann angesichts der Ge-

schwindigkeit der informationstechnischen Entwicklung nicht zuverlässig prognostiziert werden, welche Möglichkeiten dem Nutzer in Zukunft verbleiben, sich technisch selbst zu schützen.

c) Aus der Bedeutung der Nutzung informationstechnischer Systeme für die Persönlichkeitsentfaltung und aus den Persönlichkeitsgefährdungen, die mit dieser Nutzung verbunden sind, folgt ein grundrechtlich erhebliches Schutzbedürfnis. Der Einzelne ist darauf angewiesen, dass der Staat die mit Blick auf die ungehinderte Persönlichkeitsentfaltung berechtigten Erwartungen an die Integrität und Vertraulichkeit derartiger Systeme achtet. Die grundrechtlichen Gewährleistungen der Art. 10 und Art. 13 GG wie auch die bisher in der Rechtsprechung des Bundesverfassungsgerichts entwickelten Ausprägungen des allgemeinen Persönlichkeitsrechts tragen dem durch die Entwicklung der Informationstechnik entstandenen Schutzbedürfnis nicht hinreichend Rechnung.

...

d) Soweit kein hinreichender Schutz vor Persönlichkeitsgefährdungen besteht, die sich daraus ergeben, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist, trägt das allgemeine Persönlichkeitsrecht dem Schutzbedarf in seiner Lücken füllenden Funktion über seine bisher anerkannten Ausprägungen hinaus dadurch Rechnung, dass es die Integrität und Vertraulichkeit informationstechnischer Systeme gewährleistet. Dieses Recht fußt gleich dem Recht auf informationelle Selbstbestimmung auf Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG; es bewahrt den persönlichen und privaten Lebensbereich der Grundrechtsträger vor staatlichem Zugriff im Bereich der Informationstechnik auch insoweit, als auf das informationstechnische System insgesamt zugegriffen wird und nicht nur auf einzelne Kommunikationsvorgänge oder gespeicherte Daten.

aa) Allerdings bedarf nicht jedes informationstechnische System, das personenbezogene Daten erzeugen, verarbeiten oder speichern kann, des besonderen Schutzes durch eine eigenständige persönlichkeitsrechtliche Gewährleistung. Soweit ein derartiges System nach seiner technischen Konstruktion lediglich Daten mit punktuellem Bezug zu einem bestimmten Lebensbereich des Betroffenen enthält – zum Beispiel nicht vernetzte elektronische Steuerungsanlagen der Haustechnik –, unterscheidet sich ein staatlicher Zugriff auf den vorhandenen Datenbestand qualitativ nicht von anderen Datenerhebungen. In einem solchen Fall reicht der Schutz durch das Recht auf informationelle Selbstbestimmung aus, um die berechtigten Geheimhaltungsinteressen des Betroffenen zu wahren.

Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme ist hingegen anzuwenden, wenn die Eingriffsermächtigung Systeme erfasst, die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten. Eine solche Möglichkeit besteht etwa beim Zugriff auf Personalcomputer, einerlei ob sie fest installiert oder mobil betrieben werden. Nicht nur bei einer Nutzung für private Zwecke, sondern auch bei einer geschäftlichen Nutzung lässt sich aus dem Nutzungsverhalten regelmäßig auf persönliche Eigenschaften oder Vorlieben schließen. Der spezifische Grundrechtsschutz erstreckt sich ferner beispielsweise auf solche Mobiltelefone oder elektronische Terminkalender, die über einen großen Funktionsumfang verfügen und personenbezogene Daten vielfältiger Art erfassen und speichern können.

bb) Geschützt vom Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist zunächst das Interesse des Nutzers, dass die von einem vom Schutzbereich erfassten informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben. Ein Eingriff in dieses Grundrecht ist zudem dann anzunehmen, wenn die Integrität des geschützten informationstechnischen Systems angetastet wird, indem auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können; dann ist die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen.

(1) Das allgemeine Persönlichkeitsrecht in der hier behandelten Ausprägung schützt insbesondere vor einem heimlichen Zugriff, durch den die auf dem System vorhandenen Daten ganz oder zu wesentlichen Teilen ausgespäht werden können. Der Grundrechtsschutz umfasst sowohl die im Arbeitsspeicher gehaltenen als auch die temporär oder dauerhaft auf den Speichermedien des Systems abgelegten Daten. Das Grundrecht schützt auch vor Datenerhebungen mit Mitteln, die zwar technisch von den Datenverarbeitungsvorgängen des betroffenen informationstechnischen Systems unabhängig sind, aber diese Datenverarbeitungsvorgänge zum Gegenstand haben. So liegt es etwa bei einem Einsatz von sogenannten Hardware-Keyloggern oder bei einer Messung der elektromagnetischen Abstrahlung von Bildschirm oder Tastatur.

(2) Der grundrechtliche Schutz der Vertraulichkeits- und Integritätserwartung besteht unabhängig davon, ob der Zugriff auf das informations-

technische System leicht oder nur mit erheblichem Aufwand möglich ist. Eine grundrechtlich anzuerkennende Vertraulichkeits- und Integritätserwartung besteht allerdings nur, soweit der Betroffene das informationstechnische System als eigenes nutzt und deshalb den Umständen nach davon ausgehen darf, dass er allein oder zusammen mit anderen zur Nutzung berechtigten Personen über das informationstechnische System selbstbestimmt verfügt. Soweit die Nutzung des eigenen informationstechnischen Systems über informationstechnische Systeme stattfindet, die sich in der Verfügungsgewalt anderer befinden, erstreckt sich der Schutz des Nutzers auch hierauf.

2. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist nicht schrankenlos. Eingriffe können sowohl zu präventiven Zwecken als auch zur Strafverfolgung gerechtfertigt sein. Der Einzelne muss dabei nur solche Beschränkungen seines Rechts hinnehmen, die auf einer verfassungsmäßigen gesetzlichen Grundlage beruhen. Hinsichtlich der vorliegend zu überprüfenden Ermächtigung der Verfassungsschutzbehörde, präventive Maßnahmen vorzunehmen, fehlt es daran.

a) Die angegriffene Norm wird dem Gebot der Normenklarheit und Normenbestimmtheit nicht gerecht.

aa) Das Bestimmtheitsgebot findet auch im Hinblick auf das allgemeine Persönlichkeitsrecht in seinen verschiedenen Ausprägungen seine Grundlage im Rechtsstaatsprinzip (Art. 20, Art. 28 Abs. 1 GG; vgl. BVerfGE 110, 33 <53, 57, 70>; 112, 284 <301>; 113, 348 <375>; 115, 320 <365>). Es soll sicherstellen, dass der demokratisch legitimierte Parlamentsgesetzgeber die wesentlichen Entscheidungen über Grundrechtseingriffe und deren Reichweite selbst trifft, dass Regierung und Verwaltung im Gesetz steuernde und begrenzende Handlungsmaßstäbe vorfinden und dass die Gerichte die Rechtskontrolle durchführen können. Ferner sichern Klarheit und Bestimmtheit der Norm, dass der Betroffene die Rechtslage erkennen und sich auf mögliche belastende Maßnahmen einstellen kann (vgl. BVerfGE 110, 33 <52 ff.>; 113, 348 <375 ff.>). Der Gesetzgeber hat Anlass, Zweck und Grenzen des Eingriffs hinreichend bereichsspezifisch, präzise und normenklar festzulegen (vgl. BVerfGE 100, 313 <359 f., 372>; 110, 33 <53>; 113, 348 <375>; BVerfG, Beschluss vom 13. Juni 2007 – 1 BvR 1550/03 u.a. –, NJW 2007, S. 2464 <2466>).

Je nach der zu erfüllenden Aufgabe findet der Gesetzgeber unterschiedliche Möglichkeiten zur Regelung der Eingriffsvoraussetzungen vor. Die Anforderungen des Bestimmtheitsgrundsatzes richten sich auch nach

diesen Regelungsmöglichkeiten (vgl. BVerfGE 110, 33 <55 f.>; BVerfG, Beschluss vom 13. Juni 2007 – 1 BvR 1550/03 u.a. –, NJW 2007, S. 2464 <2467>). Bedient sich der Gesetzgeber unbestimmter Rechtsbegriffe, dürfen verbleibende Ungewissheiten nicht so weit gehen, dass die Vorhersehbarkeit und Justitiabilität des Handelns der durch die Normen ermächtigten staatlichen Stellen gefährdet sind (vgl. BVerfGE 21, 73 <79 f.>; 31, 255 <264>; 83, 130 <145>; 102, 254 <337>; 110, 33 <56 f.>; BVerfG, Beschluss vom 13. Juni 2007 – 1 BvR 1550/03 u.a. –, NJW 2007, S. 2464 <2467>).

...

b) § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG wahrt auch nicht den Grundsatz der Verhältnismäßigkeit. Dieser verlangt, dass ein Grundrechtseingriff einem legitimen Zweck dient und als Mittel zu diesem Zweck geeignet, erforderlich und angemessen ist (vgl. BVerfGE 109, 279 <335 ff.>; 115, 320 <345>; BVerfG, Beschluss vom 13. Juni 2007 – 1 BvR 1550/03 u.a. –, NJW 2007, S. 2464 <2468>; st. Rspr).

...

(a) Eine staatliche Datenerhebung aus komplexen informationstechnischen Systemen weist ein beträchtliches Potential für die Ausforschung der Persönlichkeit des Betroffenen auf. Dies gilt bereits für einmalige und punktuelle Zugriffe wie beispielsweise die Beschlagnahme oder Kopie von Speichermedien solcher Systeme (vgl. zu solchen Fallgestaltungen etwaBVerfGE 113, 29; 115, 166; 117, 244).

(aa) Ein solcher heimlicher Zugriff auf ein informationstechnisches System öffnet der handelnden staatlichen Stelle den Zugang zu einem Datenbestand, der herkömmliche Informationsquellen an Umfang und Vielfältigkeit bei weitem übertreffen kann. Dies liegt an der Vielzahl unterschiedlicher Nutzungsmöglichkeiten, die komplexe informationstechnische Systeme bieten und die mit der Erzeugung, Verarbeitung und Speicherung von personenbezogenen Daten verbunden sind. Insbesondere werden solche Geräte nach den gegenwärtigen Nutzungsgepflogenheiten typischerweise bewusst zum Speichern auch persönlicher Daten von gesteigerter Sensibilität, etwa in Form privater Text-, Bild- oder Tondateien, genutzt. Der verfügbare Datenbestand kann detaillierte Informationen über die persönlichen Verhältnisse und die Lebensführung des Betroffenen, die über verschiedene Kommunikationswege geführte private und geschäftliche Korrespondenz oder auch tagebuchartige persönliche Aufzeichnungen umfassen.

Ein staatlicher Zugriff auf einen derart umfassenden Datenbestand ist mit dem naheliegenden Risiko verbunden, dass die erhobenen Daten in einer Gesamtschau weitreichende Rückschlüsse auf die Persönlichkeit des Betroffenen bis hin zu einer Bildung von Verhaltens- und Kommunikationsprofilen ermöglichen.

...

(2) Der Grundrechtseingriff, der in dem heimlichen Zugriff auf ein informationstechnisches System liegt, entspricht im Rahmen einer präventiven Zielsetzung angesichts seiner Intensität nur dann dem Gebot der Angemessenheit, wenn bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen, selbst wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr schon in näherer Zukunft eintritt. Zudem muss das Gesetz, das zu einem derartigen Eingriff ermächtigt, den Grundrechtsschutz für den Betroffenen auch durch geeignete Verfahrensvorkehrungen sichern.

...

(c) Der Verhältnismäßigkeitsgrundsatz setzt einer gesetzlichen Regelung, die zum heimlichen Zugriff auf informationstechnische Systeme ermächtigt, zunächst insoweit Grenzen, als besondere Anforderungen an den Eingriffsanlass bestehen. Dieser besteht hier in der Gefahrenprävention im Rahmen der Aufgaben der Verfassungsschutzbehörde gemäß § 1 VSG.

(aa) Ein derartiger Eingriff darf nur vorgesehen werden, wenn die Eingriffsermächtigung ihn davon abhängig macht, dass tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut vorliegen. Überragend wichtig sind zunächst Leib, Leben und Freiheit der Person. Ferner sind überragend wichtig solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Hierzu zählt etwa auch die Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen.

Zum Schutz sonstiger Rechtsgüter Einzelner oder der Allgemeinheit in Situationen, in denen eine existentielle Bedrohungslage nicht besteht, ist eine staatliche Maßnahme grundsätzlich nicht angemessen, durch die – wie hier – die Persönlichkeit des Betroffenen einer weitgehenden Ausspähung durch die Ermittlungsbehörde preisgegeben wird. Zum Schutz solcher Rechtsgüter hat sich der Staat auf andere Ermittlungsbefugnisse

zu beschränken, die ihm das jeweils anwendbare Fachrecht im präventiven Bereich einräumt.

(bb) Die gesetzliche Ermächtigungsgrundlage muss weiter als Voraussetzung des heimlichen Zugriffs vorsehen, dass zumindest tatsächliche Anhaltspunkte einer konkreten Gefahr für die hinreichend gewichtigen Schutzgüter der Norm bestehen.

(1) Das Erfordernis tatsächlicher Anhaltspunkte führt dazu, dass Vermutungen oder allgemeine Erfahrungssätze allein nicht ausreichen, um den Zugriff zu rechtfertigen. Vielmehr müssen bestimmte Tatsachen festgestellt sein, die eine Gefahrenprognose tragen (vgl. BVerfGE 110, 33 <61>; 113, 348 <378>).

Diese Prognose muss auf die Entstehung einer konkreten Gefahr bezogen sein. Dies ist eine Sachlage, bei der im Einzelfall die hinreichende Wahrscheinlichkeit besteht, dass in absehbarer Zeit ohne Eingreifen des Staates ein Schaden für die Schutzgüter der Norm durch bestimmte Personen verursacht wird. Die konkrete Gefahr wird durch drei Kriterien bestimmt: den Einzelfall, die zeitliche Nähe des Umschlagens einer Gefahr in einen Schaden und den Bezug auf individuelle Personen als Verursacher. Der hier zu beurteilende Zugriff auf das informationstechnische System kann allerdings schon gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr schon in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen. Die Tatsachen müssen zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann.

Dagegen wird dem Gewicht des Grundrechtseingriffs, der in dem heimlichen Zugriff auf ein informationstechnisches System liegt, nicht hinreichend Rechnung getragen, wenn der tatsächliche Eingriffsanlass noch weitergehend in das Vorfeld einer im Einzelnen noch nicht absehbaren konkreten Gefahr für die Schutzgüter der Norm verlegt wird.

Eine Anknüpfung der Einschreitschwelle an das Vorfeldstadium ist verfassungsrechtlich angesichts der Schwere des Eingriffs nicht hinnehmbar, wenn nur ein durch relativ diffuse Anhaltspunkte für mögliche Gefahren gekennzeichnetes Geschehen bekannt ist. Die Tatsachenlage ist dann häu-

fig durch eine hohe Ambivalenz der Bedeutung einzelner Beobachtungen gekennzeichnet. Die Geschehnisse können in harmlosen Zusammenhängen verbleiben, aber auch den Beginn eines Vorgangs bilden, der in eine Gefahr mündet (vgl. zur Straftatenverhütung BVerfGE 110, 33 <59>).

...

c) Schließlich fehlt es an hinreichenden gesetzlichen Vorkehrungen, um Eingriffe in den absolut geschützten Kernbereich privater Lebensgestaltung durch Maßnahmen nach § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG zu vermeiden.

aa) Heimliche Überwachungsmaßnahmen staatlicher Stellen haben einen unantastbaren Kernbereich privater Lebensgestaltung zu wahren, dessen Schutz sich aus Art. 1 Abs. 1 GG ergibt (vgl. BVerfGE 6, 32 <41>; 27, 1 <6>; 32, 373 <378 f.>; 34, 238 <245>; 80, 367 <373>; 109, 279 <313>; 113, 348 <390>). Selbst überwiegende Interessen der Allgemeinheit können einen Eingriff in ihn nicht rechtfertigen (vgl. BVerfGE 34, 238 <245>; 109, 279 <313>). Zur Entfaltung der Persönlichkeit im Kernbereich privater Lebensgestaltung gehört die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art ohne die Angst zum Ausdruck zu bringen, dass staatliche Stellen dies überwachen (vgl. BVerfGE 109, 279 <314>).

Im Rahmen eines heimlichen Zugriffs auf ein informationstechnisches System besteht die Gefahr, dass die handelnde staatliche Stelle persönliche Daten erhebt, die dem Kernbereich zuzuordnen sind. So kann der Betroffene das System dazu nutzen, Dateien höchstpersönlichen Inhalts, etwa tagebuchartige Aufzeichnungen oder private Film- oder Tondokumente, anzulegen und zu speichern. Derartige Dateien können ebenso wie etwa schriftliche Verkörperungen des höchstpersönlichen Erlebens (dazu vgl. BVerfGE 80, 367 <373 ff.>; 109, 279 <319>) einen absoluten Schutz genießen. Zum anderen kann das System, soweit es telekommunikativen Zwecken dient, zur Übermittlung von Inhalten genutzt werden, die gleichfalls dem Kernbereich unterfallen können. Dies gilt nicht nur für Sprachtelefonate, sondern auch etwa für die Fernkommunikation mittels E-Mails oder anderer Kommunikationsdienste des Internet (vgl. BVerfGE 113, 348 <390>). Die absolut geschützten Daten können bei unterschiedlichen Arten von Zugriffen erhoben werden, etwa bei der Durchsicht von Speichermedien ebenso wie bei der Überwachung der laufenden Internetkommunikation oder gar einer Vollüberwachung der Nutzung des Zielsystems.

bb) Soll heimlich auf das informationstechnische System des Betroffenen zugegriffen werden, bedarf es besonderer gesetzlicher Vorkehrungen, die den Kernbereich der privaten Lebensgestaltung schützen.

Die Bürger nutzen zur Verwaltung ihrer persönlichen Angelegenheiten und zur Telekommunikation auch mit engen Bezugspersonen zunehmend komplexe informationstechnische Systeme, die ihnen Entfaltungsmöglichkeiten im höchstpersönlichen Bereich bieten. Angesichts dessen schafft eine Ermittlungsmaßnahme wie der Zugriff auf ein informationstechnisches System, mittels dessen die auf dem Zielsystem vorhandenen Daten umfassend erhoben werden können, gegenüber anderen Überwachungsmaßnahmen – etwa der Nutzung des Global Positioning Systems als Instrument technischer Observation (vgl. dazu BVerfGE 112, 304 <318>) – die gesteigerte Gefahr, dass Daten höchstpersönlichen Inhalts erhoben werden.

Wegen der Heimlichkeit des Zugriffs hat der Betroffene keine Möglichkeit, selbst vor oder während der Ermittlungsmaßnahme darauf hinzuwirken, dass die ermittelnde staatliche Stelle den Kernbereich seiner privaten Lebensgestaltung achtet. Diesem vollständigen Kontrollverlust ist durch besondere Regelungen zu begegnen, welche die Gefahr einer Kernbereichsverletzung durch geeignete Verfahrensvorkehrungen abschirmen.

cc) Die verfassungsrechtlichen Anforderungen an die konkrete Ausgestaltung des Kernbereichsschutzes können je nach der Art der Informationserhebung und der durch sie erfassten Informationen unterschiedlich sein.

Eine gesetzliche Ermächtigung zu einer Überwachungsmaßnahme, die den Kernbereich privater Lebensgestaltung berühren kann, hat so weitgehend wie möglich sicherzustellen, dass Daten mit Kernbereichsbezug nicht erhoben werden. Ist es – wie bei dem heimlichen Zugriff auf ein informationstechnisches System – praktisch unvermeidbar, Informationen zur Kenntnis zu nehmen, bevor ihr Kernbereichsbezug bewertet werden kann, muss für hinreichenden Schutz in der Auswertungsphase gesorgt sein. Insbesondere müssen aufgefundene und erhobene Daten mit Kernbereichsbezug unverzüglich gelöscht und ihre Verwertung ausgeschlossen werden (vgl. BVerfGE 109, 279 <318>; 113, 348 <391 f.>).

(1) Im Rahmen des heimlichen Zugriffs auf ein informationstechnisches System wird die Datenerhebung schon aus technischen Gründen zumindest überwiegend automatisiert erfolgen. Die Automatisierung erschwert es jedoch im Vergleich zu einer durch Personen durchgeführten Erhe-

bung, schon bei der Erhebung Daten mit und ohne Bezug zum Kernbereich zu unterscheiden. Technische Such- oder Ausschlussmechanismen zur Bestimmung der Kernbereichsrelevanz persönlicher Daten arbeiten nach einhelliger Auffassung der vom Senat angehörten sachkundigen Auskunftspersonen nicht so zuverlässig, dass mit ihrer Hilfe ein wirkungsvoller Kernbereichsschutz erreicht werden könnte.

Selbst wenn der Datenzugriff unmittelbar durch Personen ohne vorherige technische Aufzeichnung erfolgt, etwa bei einer persönlichen Überwachung der über das Internet geführten Sprachtelefonie, stößt ein Kernbereichsschutz schon bei der Datenerhebung auf praktische Schwierigkeiten. Bei der Durchführung einer derartigen Maßnahme ist in der Regel nicht sicher vorhersehbar, welchen Inhalt die erhobenen Daten haben werden (vgl. zur Telekommunikationsüberwachung BVerfGE 113, 348 <392>). Auch kann es Schwierigkeiten geben, die Daten inhaltlich während der Erhebung zu analysieren. So liegt es etwa bei fremdsprachlichen Textdokumenten oder Gesprächen. Auch in derartigen Fällen kann die Kernbereichsrelevanz der überwachten Vorgänge nicht stets vor oder bei der Datenerhebung abgeschätzt werden. In solchen Fällen ist es verfassungsrechtlich nicht gefordert, den Zugriff wegen des Risikos einer Kernbereichsverletzung auf der Erhebungsebene von vornherein zu unterlassen, da Grundlage des Zugriffs auf das informationstechnische System tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Schutzgut sind.

(2) Der verfassungsrechtlich gebotene Kernbereichsschutz lässt sich im Rahmen eines zweistufigen Schutzkonzepts gewährleisten.

(a) Die gesetzliche Regelung hat darauf hinzuwirken, dass die Erhebung kernbereichsrelevanter Daten soweit wie informationstechnisch und ermittlungstechnisch möglich unterbleibt (vgl. zur Telekommunikationsüberwachung BVerfGE 113, 348 <391 f.>; zur akustischen Wohnraumüberwachung BVerfGE 109, 279 <318, 324>). Insbesondere sind verfügbare informationstechnische Sicherungen einzusetzen. Gibt es im Einzelfall konkrete Anhaltspunkte dafür, dass eine bestimmte Datenerhebung den Kernbereich privater Lebensgestaltung berühren wird, so hat sie grundsätzlich zu unterbleiben. Anders liegt es, wenn zum Beispiel konkrete Anhaltspunkte dafür bestehen, dass kernbereichsbezogene Kommunikationsinhalte mit Inhalten verknüpft werden, die dem Ermittlungsziel unterfallen, um eine Überwachung zu verhindern.

(b) In vielen Fällen wird sich die Kernbereichsrelevanz der erhobenen Daten vor oder bei der Datenerhebung nicht klären lassen. Der Gesetz-

geber hat durch geeignete Verfahrensvorschriften sicherzustellen, dass dann, wenn Daten mit Bezug zum Kernbereich privater Lebensgestaltung erhoben worden sind, die Intensität der Kernbereichsverletzung und ihre Auswirkungen für die Persönlichkeit und Entfaltung des Betroffenen so gering wie möglich bleiben.

Entscheidende Bedeutung für den Schutz hat insoweit die Durchsicht der erhobenen Daten auf kernbereichsrelevante Inhalte, für die ein geeignetes Verfahren vorzusehen ist, das den Belangen des Betroffenen hinreichend Rechnung trägt. Ergibt die Durchsicht, dass kernbereichsrelevante Daten erhoben wurden, sind diese unverzüglich zu löschen. Eine Weitergabe oder Verwertung ist auszuschließen (vgl. BVerfGE 109, 279 <324>; 113, 348 <392>).

Anhang 5

Anschriften der Datenschutzbeauftragten des Bundes und der Länder

Bund	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Husarenstraße 30 53117 Bonn Verbindungsbüro Berlin: Friedrichstraße 50 10117 Berlin	Tel.: 0228/997799-0 Fax: 0228/997799-550 E-Mail: poststelle@bfdi.bund.de. Internet: www.datenschutz.bund.de
Baden-Württemberg	Der Landesbeauftragte für den Datenschutz Baden-Württemberg Postfach 10 29 32 70025 Stuttgart Urbanstraße 32 70182 Stuttgart	Tel.: 0711/615541-0 Fax: 0711/615541-15 E-Mail: poststelle@lfd.bwl.de Internet: www.baden-wuerttemberg.datenschutz.de
Bayern	Der Bayerische Landesbeauftragte für den Datenschutz Postfach 22 12 19 80502 München Wagmüllerstraße 18 80538 München	Tel.: 089/212672-0 Fax: 089/212672-50 E-Mail: poststelle@datenschutz-bayern.de Internet: www.datenschutz-bayern.de
Berlin	Berliner Beauftragter für Datenschutz und Informationsfreiheit An der Urania 4–10 10787 Berlin	Tel.: 030/13889-0 Fax: 030/2155050 E-Mail: mailbox@datenschutz-berlin.de Internet: www.datenschutz-berlin.de
Brandenburg	Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Stahnsdorfer Damm 77 14532 Kleinmachnow	Tel.: 033203/356-0 Fax: 033203/356-49 E-Mail: poststelle@lda.brandenburg.de Internet: www.lda.brandenburg.de
Bremen	Die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen Postfach 10 03 80 27503 Bremerhaven Arndtstraße 1 27570 Bremerhaven	Tel.: 0421/361-2010 Fax: 0421/469-18495 E-Mail: office@datenschutz.bremen.de Internet: www.datenschutz-bremen.de
Hamburg	Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit Klosterwall 6 (Block C) 20095 Hamburg	Tel.: 040/42854-4040 Fax: 040/42854-4000 E-Mail: mailbox@datenschutz.hamburg.de Internet: www.hamburg-datenschutz.de
Hessen	Der Hessische Datenschutzbeauftragte Postfach 31 63 65021 Wiesbaden Gustav-Stresemann-Ring 1 65189 Wiesbaden	Tel.: 0611/1408-0 Fax: 0611/1408-900 E-Mail: poststelle@datenschutz.hessen.de Internet: www.datenschutz.hessen.de

Mecklenburg-Vorpommern	Der Landesbeauftragte für Datenschutz Mecklenburg-Vorpommern Hausanschrift: Johannes-Stelling-Straße 21 19053 Schwerin Postanschrift: Schloss Schwerin 19053 Schwerin	Tel.: 0385/59494-0 Fax: 0385/59494-58 E-Mail: datenschutz@mvnet.de Internet: www.datenschutz-mv.de
Niedersachsen	Der Landesbeauftragte für den Datenschutz Niedersachsen Postfach 2 21 30002 Hannover Brühlstraße 9 30169 Hannover	Tel.: 0511/120-4500 Fax: 0511/120-4599 E-Mail: poststelle@lfd.niedersachsen.de Internet: www.lfd.niedersachsen.de
Nordrhein-Westfalen	Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen Postfach 20 04 44 40102 Düsseldorf Kavalleriestraße 2–4 40213 Düsseldorf	Tel.: 0211/38424-0 Fax: 0211/38424-10 E-Mail: poststelle@ldi.nrw.de Internet: www.ldi.nrw.de
Rheinland-Pfalz	Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz Hintere Bleiche 34 55116 Mainz	Tel.: 06131/208-2449 Fax: 06131/208-2497 E-Mail: poststelle@datenschutz.rlp.de Internet: www.datenschutz.rlp.de
Saarland	Die Landesbeauftragte für Datenschutz und Informationsfreiheit des Saarlandes Fritz-Dobisch-Straße 12 66111 Saarbrücken	Tel.: 0681/94781-0 Fax: 0681/9478129 E-Mail: poststelle@lfdi.saarland.de Internet: www.lfdi.saarland.de
Sachsen	Der Sächsische Datenschutzbeauftragte Postfach 12 09 05 01008 Dresden Bernhard-von-Lindenau-Platz 1 01067 Dresden	Tel.: 0351/493-5401 Fax: 0351/493-5490 E-Mail: saechsdsb@slt.sachsen.de Internet: www.datenschutz.sachsen.de
Sachsen-Anhalt	Landesbeauftragter für den Datenschutz Sachsen-Anhalt Postfach 19 47 39009 Magdeburg Leiterstraße 9 39104 Magdeburg	Tel.: 0391/81803-0 Fax: 0391/81803-33 E-Mail: poststelle@lfd.sachsen-anhalt.de Internet: www.datenschutz.sachsen-anhalt.de
Schleswig-Holstein	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein Postfach 71 16 24171 Kiel Holstenstraße 98 24103 Kiel	Tel.: 0431/988-1200 Fax: 0431/988-1223 E-Mail: mail@datenschutzzentrum.de Internet: www.datenschutzzentrum.de
Thüringen	Der Thüringer Landesbeauftragte für den Datenschutz Postfach 90 04 55 99107 Erfurt Jürgen-Fuchs-Straße 1 99096 Erfurt	Tel.: 0361/377-1900 Fax: 0361/377-1904 E-Mail: poststelle@datenschutz.thueringen.de Internet: www.thueringen.de/datenschutz

Anhang 6

Anschriften der Aufsichtsbehörden für den nicht-öffentlichen Bereich

Baden-Württemberg	Innenministerium Baden-Württemberg - Referat Datenschutz - Postfach 10 24 43 70020 Stuttgart Dorotheenstraße 6 70173 Stuttgart	Tel.: 0711/231-4 Fax: 0711/231-5000 E-Mail: datenschutz@im.bwl.de Internet: www.im.baden-wuerttemberg.de
Bayern	Bayerisches Landesamt für Datenschutzaufsicht in der Regierung von Mittelfranken Promenade 27 (Schloss) 91522 Ansbach	Tel.: 0981/53-1301 Fax: 0981/53-5301 E-Mail: datenschutz@reg-mfr.bayern.de Internet: www.regierung.mittelfranken.bayern.de
Berlin	Berliner Beauftragter für Datenschutz und Informationsfreiheit An der Urania 4–10 10787 Berlin	Tel.: 030/13889-0 Fax: 030/2155050 E-Mail: mailbox@datenschutz-berlin.de Internet: www.datenschutz-berlin.de
Brandenburg	Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Stahnsdorfer Damm 77 14532 Kleinmachnow	Tel.: 033203/356-0 Fax: 033203/356-49 E-Mail: poststelle@lda.brandenburg.de Internet: www.lda.brandenburg.de
Bremen	Die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen Postfach 10 03 80 27503 Bremerhaven Arndtstraße 1 27570 Bremerhaven	Tel.: 0421/361-2010 Fax: 0421/496-18495 E-Mail: office@datenschutz.bremen.de Internet: www.datenschutz-bremen.de
Hamburg	Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit Klosterwall 6 (Block C) 20095 Hamburg	Tel.: 040/42854-4040 Fax: 040/42854-4000 E-Mail: mailbox@datenschutz.hamburg.de Internet: www.hamburg.datenschutz.de
Hessen	Regierungspräsidium Darmstadt Dezernat Datenschutz - Kollegiengebäude - Luisenplatz 2 64283 Darmstadt	Tel.: 06151/12-0 Fax: 06151/12-5794 E-Mail: datenschutz@rpda.hessen.de Internet: www.rp-darmstadt.hessen.de
Mecklenburg-Vorpommern	Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern Hausanschrift: Johannes–Stelling–Straße 21 19053 Schwerin Postanschrift: Schloss Schwerin 19053 Schwerin	Tel.: 0385/59494-0 Fax: 0385/59494-58 E-Mail: datenschutz@mvnet.de Internet: www.datenschutz.m-v.de

Niedersachsen	Der Landesbeauftragte für den Datenschutz Niedersachsen Postfach 221 30002 Hannover	Tel.: 0511/120-4500 Fax: 0511/120-4599 E-Mail: poststelle@lfd.niedersachsen.de Internet: www.lfd.niedersachsen.de
Nordrhein-Westfalen	Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen Kavalleriestraße 2-4 40213 Düsseldorf	Tel.: 0211/384240 Fax: 0211/3842410 E-Mail: poststelle@ldi.nrw.de Internet: www.ldi.nrw.de
Rheinland-Pfalz	Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz Hintere Bleiche 34 55116 Mainz	Tel.: 06131/208-2449 Fax: 06131/208-2497 E-Mail: poststelle@datenschutz.rlp.de Internet: www.datenschutz.rlp.de
Saarland	Ministerium für Inneres und Europaangelegenheiten – Abt. B - Franz-Josef-Röder-Straße 21 66119 Saarbrücken Postfach 10 24 41 66024 Saarbrücken	Tel.: 0681/501-00 Fax: 0681/501-2699 E-Mail: datenschutz@innen.saarland.de Internet: www.innen-saarland.de
Sachsen	Der Sächsische Datenschutzbeauftragte Bernhard-von-Lindenau-Platz 1 01067 Dresden	Tel.: 0351/493-5401 Fax: 0351/493-5490 E-Mail: saechsdsb@slt.sachsen.de Internet: www.datenschutz.sachsen.de
Sachsen-Anhalt	Landesverwaltungsamt Sachsen-Anhalt Referat 106 (Justiziariat) Postfach 20 02 56 06003 Halle (Saale) Ernst-Karmieth-Straße 2 06114 Halle (Saale)	Tel.: 0345/5140 Fax: 0345/5141444 E-Mail: poststelle@lvwa.sachsen-anhalt.de Internet: www.landesverwaltungsamt. sachsen-anhalt.de
Schleswig-Holstein	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein Postfach 71 16 24171 Kiel Holstenstraße 98 24103 Kiel	Tel.: 0431/9881200 Fax: 0431/9881223 E-Mail: mail@datenschutzzentrum.de Internet: www.datenschutzzentrum.de
Thüringen	Thüringer Landesverwaltungsamt - Referat 200 - Weimarplatz 4 99423 Weimar	Tel.: 0361/377-0 Fax: 0361/377-3746 E-Mail: poststelle@tlvwa.thueringen.de

Anhang 7

Anschriften der Rundfunkbeauftragten für den Datenschutz

Bayerischer Rundfunk Datenschutzbeauftragte Rundfunkplatz 1 80330 München	Tel.: 089/5900-3045 Fax: 089/5900-2409 E-Mail: datenschutz@br-online.de
Deutsche Welle Datenschutzbeauftragter Kurt-Schumacher-Straße 53113 Bonn	Tel.: 0228/429-2123 Fax: 0228/429-2195
DeutschlandRadio Datenschutzbeauftragter Raderberggürtel 40 50968 Köln	Tel.: 0221/345-3501 Fax: 0221/345-4801
Hessischer Rundfunk Datenschutzbeauftragter Bertramstraße 8 60320 Frankfurt	Tel.: 069/155-2541 Fax: 069/155-4175 E-Mail: datenschutz@hr-online.de
Mitteldeutscher Rundfunk Datenschutzbeauftragter Kantstraße 71–73 04360 Leipzig	Tel.: 0341/300-7508 Fax: 0341/300-7548 E-Mail: Ralf.Lehmann@mdr.de
Norddeutscher Rundfunk Datenschutzbeauftragter Rothenbaumchaussee 132 20149 Hamburg	Tel.: 040/4156-2232 Fax: 040/4156-3697 E-Mail: datenschutz@ndr.de
Radio Bremen Datenschutzbeauftragter Heinrich-Hertz-Straße 13 28329 Bremen	Tel.: 0421/246-41026 Fax: 0421/246-41097
Rundfunk Berlin-Brandenburg Datenschutzbeauftragte Masurenallee 8–14 14057 Berlin	Tel.: 030/97 99 36 04 00 Fax: 030/97 99 36 01 09
Saarländischer Rundfunk Datenschutzbeauftragter Funkhaus Halberg 66100 Saarbrücken	Tel.: 0681/602-2050 Fax: 0681/602-2057
Südwestrundfunk Datenschutzbeauftragter Neckarstraße 230 70190 Stuttgart	Tel.: 0711/929-3014 Fax: 0711/929-3019 E-Mail: datenschutz@swr.de
Westdeutscher Rundfunk Datenschutzbeauftragter Apellhofplatz 1 50667 Köln	Tel.: 0221/220-8530 Fax: 0221/220-8533 E-Mail: ds-wdr@wdr.de

Zweites Deutsches Fernsehen Datenschutzbeauftragter ZDF-Straße 1 55127 Mainz	Tel.: 06131/70-5434 Fax: 06131/70-5452 E-Mail: datenschutz@zdf.de
Gebühreneinzugszentrale (GEZ) Datenschutzbeauftragte Freimersdorfer Weg 6 50829 Köln	Tel. : 0221/5061-2632 Fax : 0221/5061-2708 E-Mail : datenschutz@gez.de

Anhang 8

Informationen zum Datenschutz im Internet

Die Homepage des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erreichen Sie unter www.datenschutz.bund.de.

Der Besucher kann zwischen den Beiträgen zum Datenschutz oder zur Informationsfreiheit wählen.
Hier finden Sie umfassende Informationen zu dem gesamten Themenspektrum des Datenschutzes und der Informationsfreiheit sowie alle Veröffentlichungen des Bundesbeauftragten, Entschließungen der internationalen, europäischen und nationalen Datenschutzkonferenzen sowie Anschriften und weitere interessante Links.
Fragen rund um das Thema Datenschutz können Sie in dem virtuellen Datenschutzforum unter www.datenschutzforum.bund.de mit anderen Interessierten diskutieren.
Daneben können Informationen zum Datenschutz auch beim **Virtuellen Datenschutzbüro** unter der Adresse www.datenschutz.de abgerufen werden. Das Virtuelle Datenschutzbüro ist eine im Internet betriebene zentrale Informations- und Anlaufstelle für Datenschutzfragen, die von zahlreichen offiziellen Datenschutzinstitutionen (Projektpartnern) mitgetragen wird. Das Projekt wurde vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein initiiert und aufgebaut. Es ist Portal und Ansprechstelle im Internet für alle Bürgerinnen und Bürger, Experten und Datenschutzinstitutionen. Projektpartner sind neben dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit auch die Datenschutzbeauftragten der meisten Bundesländer, die Datenschutzbeauftragten der Evangelischen Kirche sowie der Norddeutschen Bistümer der Katholischen Kirche sowie Datenschutzbeauftragte aus Kanada, den Niederlanden, der Schweiz, Liechtenstein, Polen und der Slowakei.

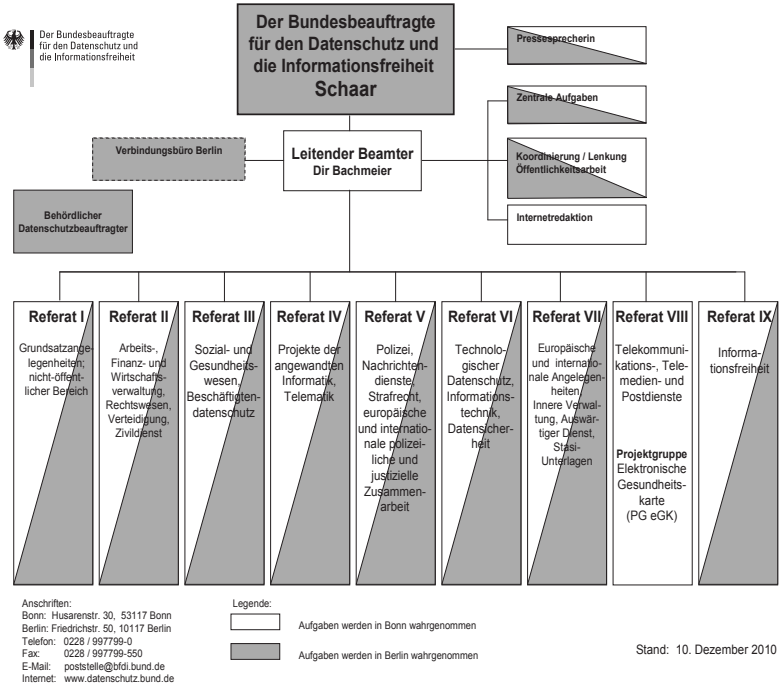
Das Virtuelle Datenschutzbüro bietet u.a.:

- Informationen zu allen Fragen rund um den Datenschutz,
- Diskussionsforen zu aktuellen Datenschutzthemen,
- Antworten zu den häufigsten Fragen von Anwendern,
- eine Plattform für die Zusammenarbeit der Datenschützer weltweit.

Anhang 9

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Organisationsübersicht (Stand: Dezember 2010)



Anschriften:
Bonn: Husarenstr. 30, 53117 Bonn
Berlin: Friedrichstr. 50, 10117 Berlin
Telefon: 0228 / 997799-0
Fax: 0228 / 997799-550
E-Mail: poststelle@bfdi.bund.de
Internet: www.datenschutz.bund.de

Legende:
Aufgaben werden in Bonn wahrgenommen
Aufgaben werden in Berlin wahrgenommen

Stand: 10. Dezember 2010

Der Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit
Husarenstraße 30
D-53117 Bonn

Tel. +49 (0) 228 997799-0
Fax +49 (0) 228 997799-550
E-Mail: poststelle@bfdi.bund.de
Internet: www.datenschutz.bund.de