Bundesministerium des Innern
Alt-Moabit 101 D
10559 Berlin
Referat V 7

Gesetz zur Änderung des

Bundesdatenschutzgesetzes (BDSG) und anderer Gesetze[*)]

Synopse zu dem am 23. Mai 2001 in Kraft tretenden Änderungen (nur) des BDSG

(mit *Begründung des Regierungsentwurfs*, BT-Drs. 14/4329, und
Begründung zur Beschlussempfehlung des BT-Innenausschusses vom 04.04.2001, BT-Drs. 14/5793)

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

Artikel 1

Änderung des Bundesdatenschutzgesetzes

Begründung: A. Allgemeines

1. Allgemeine Vorgaben

1.1 Zielsetzung

Der Gesetzentwurf dient der Anpassung des Bundesdatenschutzgesetzes (BDSG) an die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Okto-ber 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG L Nr. 281 vom 23. November 1995, S. 31 ff; im folgenden: Richtlinie).

Die Richtlinie ist am 13. Dezember 1995 in Kraft getreten.

Die Richtlinie konkretisiert und ergänzt die Grundsätze der Datenschutzkonvention des Europarates von 1981 (BGBl. 1985 II, S. 538 ff). Sie erweitert die Informationsrechte des Bürgers und verpflichtet die Mitgliedstaaten zur Einrichtung staatlicher Kontrollstellen, die die Einhaltung der in Umsetzung der Richtlinie geschaffenen nationalen Vorschriften überwachen.

Durch die Richtlinie wird ein einheitliches Datenschutzniveau für die Ausführung und Anwendung des Gemeinschaftsrechts durch die Mitgliedstaaten der EU geschaffen. Daher ist der innergemeinschaftliche Datenverkehr innerhalb des Anwendungsbereichs der Richtlinie künftig dem inländischen gleichzustellen. Für den Austausch personenbezogener Daten mit Drittstaaten sieht die Richtlinie ebenfalls die grundsätzliche Geltung der gemeinschaftlichen Standards vor, ohne den Wirtschaftsverkehr unangemessen zu beeinträchtigen.

1.2 Gesetzgebungskompetenz

Eine ausdrückliche Kompetenz des Bundes zu einer umfassenden Regelung der Querschnittsmaterie des Datenschutzes enthält das Grundgesetz nicht. Die Gesetzgebungskompetenz des Bundes ergibt sich aber im Rückgriff auf die dem Bund zustehenden Gesetzgebungskompetenzen für verschiedene Bereiche, die für den Datenschutz von Bedeutung sind. So folgt im Anwendungsbereich der öffentlichen Verwaltung die Gesetzgebungsbefugnis aus der Annexkompetenz des Verwaltungsverfahrens zu den jeweiligen Sachkompetenzen der Artikel 73 bis 75 des Grundgesetzes (GG). Bundesrechtliche Datenschutzbestimmungen können daher für die Verwaltungstätigkeit des Bundes sowie für die der Länder, soweit diese Bundesrecht ausführen, erlassen werden.

Für die gesetzliche Regelung im nicht-öffentlichen Bereich beruht die Gesetzgebungskompetenz des Bundes auf der jeweiligen Sachkompetenz, also insbesondere auf Artikel 74 Nr. 1, 11 und 12 GG. Im Hinblick auf die Gegenstände der konkurrierenden Gesetzgebung ist maßgeblich, dass ein unterschiedlicher Datenschutzstandard im nicht-öffentlichen Bereich gravierende Auswirkungen auf die hierdurch in erster Linie betroffene Wirtschaft hätte, die in ihrer unternehmerischen Tätigkeit durch im Kern unterschiedliche Länderregelungen gehemmt würde. Eine einheitliche Regelung durch den Bund zur Erzielung eines einheitlichen Datenschutzstandards ist daher zur Wahrung der Rechts- und Wirtschaftseinheit im gesamtstaatlichen Interesse zwingend erforderlich.

1.3 Kosten

Der Gesetzentwurf ist darauf ausgerichtet, die Richtlinie in dem erforderlichen Umfang umzusetzen und dabei von den zur Verfügung stehenden Optionen in einer für Bund, Länder, Gemeinden und Wirtschaft möglichst kostengünstigen Weise Gebrauch zu machen. Die geplante Regelung wird voraussichtlich durch folgende Änderungen zu Mehrbelastungen der Wirtschaft und Verwaltung führen:

durch die Aufnahme des Grundsatzes der Datenvermeidung und -sparsamkeit und des Vorrangs pseudonymer und anonymer Formen der Datenverarbeitung (§ 3 a), die Einführung von Informationspflichten im Rahmen der Erhebung personenbezogener Daten beim Betroffenen auch im nicht-öffentlichen Bereich (§ 4 Abs. 3), die Verpflichtung zur Kenntlichmachung der Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (§ 6 b), die prinzipielle Benachrichtigungspflicht gegenüber dem Betroffenen im öffentlichen Bereich (§ 19 a), die Einführung eines Auskunftsrechts bei sog. automatisierten Einzelentscheidungen (§ 6 a Abs. 3), die Modifizierung der bestehenden Meldepflicht für nicht-öffentliche Stellen, die Einführung der sog. Vorabkontrolle für bestimmte automatisierte Verarbeitungen (§ 4 d Abs. 5) sowie die obligatorische Bestellung von behördlichen Datenschutzbeauftragten im öffentlichen Bereich.

B. Im Einzelnen:

Durch die Einführung des Grundsatzes der Datenvermeidung und -sparsamkeit in § 3 a soll Einfluss auf die Gestaltung der Systemstrukturen, in denen personenbezogene Daten erhoben und verarbeitet werden, genommen werden. Insbesondere in Verbindung mit dem Vorrang pseudonymer und anonymer Formen der Datenverarbeitung sind daher Mehrausgaben im Bereich der EDV sowohl für die Unternehmen als auch für die Verwaltung vorstellbar. Da der Grundsatz der Datenvermeidung und -sparsamkeit erstmalig in das allgemeine Datenschutzrecht aufgenommen wird, sind konkrete Aussagen hierzu jedoch derzeit nicht möglich.

Im Gegensatz zur bisherigen Rechtslage sind nunmehr auch nicht-öffentliche Stellen, die personenbezogene Daten beim Betroffenen erheben, nach § 4 Abs. 3 diesem gegenüber u.a. zur Nennung der Identität der verantwortlichen Stelle sowie der Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung verpflichtet. Die Rechtsänderung beruht auf den Vorgaben von Artikel 10 der Richtlinie. Betroffen sind alle Wirtschaftsunternehmen, die personenbezogene Daten beim Betroffenen erheben. Es ist davon auszugehen, dass die Unternehmen ihrer Verpflichtung vorwiegend durch Ergänzungen ihrer formularmäßigen Hinweise nachkommen werden.

Die Pflicht zur Kenntlichmachung des Umstandes der Beobachtung und der verantwortlichen Stelle im Rahmen der Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (§ 6 b Abs. 2) betrifft sowohl die Unternehmen als auch die Verwaltung. Da diese Kenntlichmachungspflicht nach den bereits bestehenden Erfahrungen im Regelfall durch entsprechende Hinweisschilder erfüllt wird, kann davon ausgegangen werden, dass die hierdurch verursachte Mehrbelastung insgesamt gering bleiben dürfte.

Die aufgrund von Artikel 11 der Richtlinie einzuführende Benachrichtigungspflicht des Betroffenen im öffentlichen Bereich über die Speicherung bzw. Übermittlung seiner Daten wird sich angesichts des weitgehenden Ausnahmekatalogs (vgl. § 19 a Abs. 2) für die öffentlichen Stellen nahezu kostenneutral auswirken.

Die Richtlinie verpflichtet in Artikel 12 Buchstabe a dritter Spiegelstrich zur Schaffung eines Auskunftsrechts über den „logischen Aufbau automatisierter Verarbeitungen“. Dieses neue Auskunftsrecht war gemäß der Richtlinie „zumindest im Fall automatisierter Entscheidungen“ zwingend umzusetzen. Nur in diesem Bereich wurde es umgesetzt durch die Einstellung in § 6 a Abs. 3. Betroffen sind hiervon die öffentliche Verwaltung und alle Wirtschaftsunternehmen, die automatisierte Einzelentscheidungen im Sinne des § 6 a treffen. In der Vorschrift werden alle Ausnahmen vom Verbot derartiger automatisierter Einzelentscheidungen ausgeschöpft (§ 6 a Abs. 2). Der Anwendungsbereich der Vorschrift und somit auch des Auskunftsrechts wird daher eher gering sein, die zu erwartende Mehrbelastung der öffentlichen Verwaltung und der betroffenen Wirtschaftsunternehmen dürfte insgesamt gering bleiben.

Im Hinblick auf die Meldepflicht für automatisierte Verarbeitungen durch Wirtschaftsunternehmen macht der Gesetzentwurf - ausgehend von dem in Artikel 18 Abs. 1 der Richtlinie zwingend vorgeschriebenen Prinzip der allgemeinen Meldepflicht - Gebrauch von der Option, von der Meldepflicht abzusehen, sofern entweder ein betrieblicher/behördlicher Datenschutzbeauftragter bestellt wird oder es sich um eine sog. weniger beeinträchtigende Verarbeitung handelt (Artikel 18 Abs. 2 erster und zweiter Spiegelstrich der Richtlinie). Der Entwurf zielt auf die möglichst weitgehende Abschaffung von Meldepflichten und setzt daher beide Ausnahmen von der Meldepflicht um (§ 4 d Abs. 2 und 3). Für den öffentlichen Bereich hat dies die völlige Abschaffung der Meldepflicht und damit auch den Verzicht auf das beim Bundesbeauftragten für den Datenschutz eingerichtete Register der bei öffentlichen Stellen des Bundes geführten automatisierten Dateien zur Folge. Im nicht-öffentlichen Bereich verbleibt es insoweit bei der derzeit bereits geltenden Verpflich-

tung, betriebliche Datenschutzbeauftragte zu bestellen, soweit mehr als vier Arbeitnehmer mit automatisierter Datenverarbeitung beschäftigt sind. In diesem Fall entfällt zukünftig die Meldepflicht. Zur Vermeidung der Meldepflicht kann ein betrieblicher Datenschutzbeauftragter auch auf freiwilliger Basis bestellt werden (§ 4 d Abs. 2 Satz 2). In den übrigen Fällen besteht eine Meldepflicht, sofern es sich nicht um „weniger beeinträchtigende Verarbeitungen“ im Sinne des Artikel 18 Abs. 2 erster Spiegelstrich der Richtlinie handelt. Dies ist der Fall, wenn personenbezogene Daten für eigene Zwecke erhoben, verarbeitet oder genutzt werden, hierbei höchstens vier Arbeitnehmer beschäftigt sind und entweder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses dient (§ 4 d Abs. 3).

Diese Voraussetzung wird regelmäßig bei der Datenverarbeitung einer Reihe von selbständig Berufstätigen, etwa Architekten, Ärzten, Apothekern u.ä., vorliegen.

Die in § 4 d Abs. 5 vorgesehene Vorabkontrolle betrifft besonders risikoreiche Datenverarbeitungen. Da es sich bei der Vorabkontrolle um eine neue Einrichtung handelt, ist der damit verbundene Zeit- und Kostenaufwand noch nicht absehbar. Zuständig für die Durchführung der Vorabkontrolle ist der betriebliche Datenschutzbeauftragte.

Der Arbeitsaufwand des betrieblichen Datenschutzbeauftragten wird durch zwei neue Aufgaben vermutlich nur geringfügig erhöht: Die bereits erwähnte Vorabkontrolle sowie die ebenfalls durch den betrieblichen Datenschutzbeauftragten zu erfüllende Aufgabe nach § 4 g Abs. 2 Satz 2, Angaben zu automatisierten Verarbeitungen „auf Antrag jedermann in geeigneter Weise verfügbar zu machen“. Diese zweite Aufgabe beruht auf Artikel 21 Abs. 3 der Richtlinie. Sie obliegt auch dem behördlichen Datenschutzbeauftragten, der bereits jetzt in allen obersten Bundesbehörden ohne gesetzliche Verpflichtung existiert. Mit Blick auf die vergleichbaren Regelungen in § 38 Abs. 2 Satz 3 und § 26 Abs. 5 Satz 4 BDSG a.F. (Einsichtsrecht in das Register der Aufsichtsbehörden und des Bundesbeauftragten für den Datenschutz), die in der Praxis kaum eine Rolle gespielt haben, ist insoweit nicht von einer wesentlichen Mehrbelastung der betrieblichen bzw. behördlichen Datenschutzbeauftragten auszugehen. Die Auskunft kann im übrigen in pauschalierter Form erfolgen.

Die obligatorische Bestellung von Datenschutzbeauftragten im öffentlichen Bereich wird aufgrund der besonderen Struktur des Bundesministeriums der Verteidigung und seines Geschäftsbereichs dort zu zusätzlichem Personalaufwand und somit zu erhöhten Kosten führen. Da - unabhängig von der Anzahl der Arbeitnehmer - künftig betriebliche Datenschutzbeauftragte zu bestellen sind, wenn nicht-öffentliche Stellen zur Durchführung einer Vorabkontrolle verpflichtet sind oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung oder der anonymisierten Übermittlung erheben, verarbeiten oder nutzen (§ 4 f Abs. 1 Satz 6), kann es auch in diesem Bereich zu Mehrkosten kommen.

2. Wesentliche Inhalte des Gesetzentwurfs

2.1 Grundzüge der Novellierung

Der Anwendungsbereich der Richtlinie ist beschränkt auf den Geltungsbereich des EG-Vertrages. Die Datenverarbeitung von Polizei- und Nachrichtendiensten ist daher von der Richtlinie nicht unmittelbar berührt. Allerdings erscheint es nicht sinnvoll, eine lediglich auf den Geltungsbereich des EG-Vertrages beschränkte Anpassung des Bundesdatenschutzgesetzes vorzunehmen. Sonst würden unterschiedliche Regelungen gelten, je nachdem, ob Gemeinschaftsrecht oder ausschließlich deutsches Recht auszuführen und anzuwenden ist. Dies wäre mit dem Querschnittscharakter und der subsidiären Geltung des Bundesdatenschutzgesetzes nicht vereinbar.

Die Transparenz der Datenverarbeitung für den Bürger wurde u.a. erhöht durch die Ausdehnung der Benachrichtigungspflicht des Betroffenen von der Speicherung / Weitergabe seiner Daten auch auf den öffentlichen Bereich, durch eine grundsätzliche Informationspflicht des Betroffenen bei der Erhebung seiner Daten auch im nicht-öffent-lichen Bereich und eine geringfügige Erweiterung des Auskunftsrechts. Ebenfalls der Bürgerfreundlichkeit dient die Vorschrift des § 6 a, wonach belastende Entscheidungen, die aufgrund von Persönlichkeitsprofilen ohne zusätzliche Überprüfung durch einen Menschen erfolgen, grundsätzlich verboten sind.

Die Richtlinie sieht eine Reihe von Restriktionen im Zusammenhang mit der Verarbeitung sog. sensitiver Daten vor, die den Bürger in diesem empfindlichen Bereich besonders schützen sollen. Die Richtlinie versteht unter sensitiven Daten solche, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben. In Umsetzung der Vorgaben der Richtlinie unterliegt nun der Umgang mit diesen Daten besonderen Einschränkungen sowohl im öffentlichen als auch im nicht-öffentlichen Bereich.

Wichtig unter dem Aspekt der Erhaltung der unternehmerischen Freiheit und möglichst uneingeschränkter wirtschaftlicher Betätigung ist die Neuregelung der Übermittlung personenbezogener Daten in Drittstaaten. Übermittlungen personenbezogener Daten dürfen grundsätzlich nur bei Vorliegen eines angemessenen Datenschutzniveaus im Drittstaat vorgenommen werden. Durch einen breiten Ausnahmekatalog wird aber sichergestellt, dass der Wirtschaftsverkehr mit Drittstaaten nicht unangemessen beeinträchtigt wird.

Der Entbürokratisierung dient die Neuregelung der Meldepflicht automatisierter Verarbeitungen. Diese ist dahingehend modifiziert worden, dass die in der Richtlinie vorgesehene Möglichkeit der Einschränkung der allgemeinen Meldepflicht weitestgehend genutzt wurde. So entfällt nach der Regelung des § 4 d Abs. 2 die Meldepflicht, wenn die speichernde Stelle einen internen Datenschutzbeauftragten bestellt hat und im Falle des Vorliegens einer weniger beeinträchtigenden Verarbeitung (§ 4 d Abs. 3). Da durch § 4 f Abs. 1 der behördliche Datenschutzbeauftragte als obligatorische Institution eingeführt wird, kann die Meldepflicht im öffentlichen Bereich vollständig entfallen.

Die Wahrung des sog. Medienprivilegs wird in weitem Umfang gewährleistet. Die durch die Richtlinie erforderlich gewordene Erweiterung des Anwendungsbereichs für Unternehmen der Presse wurde restriktiv vorgenommen.

2.2 Die wesentlichen Änderungen aufgrund der Richtlinie im einzelnen

– Der Anwendungsbereich des Bundesdatenschutzgesetzes war durch die Vorschrift des § 1 Abs. 5 zu ergänzen: Diese betrifft zum einen die Datenverarbeitung innerhalb der Europäischen Union. Das Bundesdatenschutzgesetz kommt hier nicht zur Anwendung, wenn die Verarbeitung personenbezogener Daten durch eine verantwortliche Stelle eines anderen Mitgliedstaates der Europäischen Union im Inland ausgeführt wird. Als Ausnahme dieser Regelung findet das Bundesdatenschutzgesetz aber Anwendung, sofern die verantwortliche Stelle eine Niederlassung im Inland unterhält. Zum anderen soll mit der Vorschrift verhindert werden, dass ein möglicherweise geringerer Datenschutzstandard als der in den Mitgliedstaaten der Europäischen Union vorhandene in den Fällen zur Geltung kommt, in denen Datenerhebungen, -verarbeitungen oder -nutzungen innerhalb der Europäischen Union durch außerhalb der Europäischen Union belegene speichernde Stellen vorgenommen werden.

  Darüber hinaus waren die Kriterien für den sachlichen Anwendungsbereich des Bundesdatenschutzgesetzes insofern in Übereinstimmung mit Artikel 3 Abs. 1 der Richtlinie zu bringen, als es bei automatisierten Verarbeitungen nicht mehr auf den Dateibegriff ankommt. Das Kriterium der Datei ist nur noch von Bedeutung, soweit es um die nicht-automatisierte Verarbeitung personenbezogener Daten geht.

– Da die Richtlinie die Erhebung personenbezogener Daten als Teil der Verarbeitung begreift, das Bundesdatenschutzgesetz bisher aber nur die Erhebung für den öffentlichen Bereich regelt, bedurfte es der Einführung eines Gesetzesvorbehaltes auch für die Erhebung im nicht-öffentlichen Bereich.

– Im Gegensatz zur bisherigen Rechtslage kommt dem Begriff des "Empfängers" nunmehr neben dem des "Dritten" eigenständige Bedeutung zu. Er war daher in § 3 Abs. 8 zu definieren, seine bisherige Verwendung im Bundesdatenschutzgesetz anzupassen.

– Die Übermittlung personenbezogener Daten in Drittstaaten wurde in § 4 b und § 4 c neu geregelt. Diese Vorschriften sollen zum einen ein koordiniertes Verhalten der Mitgliedstaaten beim Transfer in Drittstaaten sicherstellen und zum anderen - durch einen breiten Katalog von Ausnahmebestimmungen - dafür Sorge tragen, dass der Wirtschaftsverkehr mit Drittstaaten nicht unangemessen beeinträchtigt wird.

  Da nach Umsetzung der Richtlinie durch die Mitgliedstaaten der Europäischen Union innerhalb des Anwendungsbereichs der Richtlinie von einem angemessenen Datenschutzniveau innerhalb der Europäischen Union auszugehen ist, gelten insoweit die §§ 15, 16 und 28 ff.

– In den neu eingefügten §§ 4 d und 4 e ist die Meldepflicht für automatisierte Verarbeitungen öffentlicher und nicht-öffentlicher Stellen geregelt.

  Nach der Regelung des § 4 d Abs. 2 und 3 entfällt die Meldepflicht, wenn die verantwortliche Stelle einen Datenschutzbeauftragten bestellt hat oder eine weniger beeinträchtigende Verarbeitung vorliegt. Damit kann die Meldepflicht im öffentlichen Bereich vollständig entfallen, da durch § 4 f Abs. 1 der behördliche Datenschutzbeauftragte als obligatorische Institution eingeführt wird. Neu ist die sog. Vorabkontrolle, d.h. bestimmte automatisierte Verarbeitungen werden vor Inbetriebnahme einer Prüfung durch den Datenschutzbeauftragten unterzogen.

- Die neue Vorschrift des § 6 a beinhaltet die Regelung der sog. automatisierten Einzelentscheidung. Durch die Vorschrift soll verhindert werden, dass Entscheidungen ausschließlich aufgrund von automatisiert erstellten Persönlichkeitsprofilen getroffen werden, ohne dass eine Person den Sachverhalt erneut überprüft hat.
- Die Regelungen über die Erhebung und zweckändernde Verarbeitung personenbezogener Daten waren sowohl im öffentlichen als auch im nicht-öffentlichen Bereich um Sonderregelungen hinsichtlich sog. sensitiver Daten zu ergänzen (§§ 13, 14 Abs. 5, 28 Abs. 6 und 7, 29 Abs. 5, 30 Abs. 5). Entsprechendes gilt für die Voraussetzungen der Einwilligung, § 4 a Abs. 3.
- Der neu geschaffene § 19 a führt eine Benachrichtigungspflicht im öffentlichen Bereich für die Fälle ein, in denen Daten nicht beim Betroffenen selbst erhoben werden.
- Da die Richtlinie keine Beschränkung der Datenschutzkontrolle auf eine Anlasskontrolle vorsieht, wie sie in § 38 Abs. 1 und § 24 Abs. 1 Satz 2 a.F. geregelt war, waren die entsprechenden Einschränkungen zu streichen.
- Die neue Vorschrift des § 38 a beinhaltet Regelungen im Zusammenhang mit den sog. Verhaltensregeln zur Förderung der ordnungsgemäßen Durchführung datenschutzrechtlicher Regelungen, die u.a. eine Vereinheitlichung derartiger interner Regeln bewirken sollen. Berufsverbände und ähnliche Vereinigungen erhalten die Möglichkeit, von ihnen erarbeitete Verhaltensregeln der Aufsichtsbehörde zu unterbreiten. Diese überprüft die Vereinbarkeit der Entwürfe mit dem geltenden Datenschutzrecht.
- Die Vorschrift des § 41, die die Verarbeitung und Nutzung personenbezogener Daten durch Medien regelt, ist als Rahmenvorschrift für die Landesgesetzgebung ausgestaltet worden. Der Anwendungsbereich der Datenschutzbestimmungen für die Medien ist auf die Vorschriften über die Haftung (insoweit nur eingeschränkt) und die Verhaltensregeln zur Förderung der Durchführung datenschutzrechtlicher Regelungen erweitert worden. Gleichzeitig war der Anwendungsbereich des sog. Medienprivilegs zu erweitern, da nunmehr auch die Verarbeitung personenbezogener Daten zu literarischen Zwecken hiervon erfasst wird.
- Die Anlage zu § 9 wurde gestrafft, um die Anforderungen der Richtlinie ergänzt, sprachlich überarbeitet sowie den heutigen Gegebenheiten der Informations- und Kommunikationstechnik angepasst.

2.3 Sonstige wesentliche Änderungen des Bundesdatenschutzgesetzes

Neben den unmittelbar durch die Umsetzung der Datenschutzrichtlinie bedingten Änderungen des Bundesdatenschutzgesetzes sieht diese Novelle folgende neue Regelungen vor:

Der Grundsatz der Datenvermeidung und -sparsamkeit (§ 3 a) besagt, dass sich die Gestaltung und Auswahl von Systemen der Datenverarbeitungsanlagen an dem Ziel auszurichten hat, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten. Die Regelung soll dazu führen, dass durch den gezielten Einsatz datenschutzfreundlicher Technik die Gefahren für das informationelle Selbstbestimmungsrecht der Betroffenen reduziert werden.

Die in weiten Bereichen durch öffentliche und nicht-öffentliche Stellen bereits durchgeführte Videoüberwachung öffentlich zugänglicher Räume erhält durch die Vorschrift des § 6 b eine gesetzliche Grundlage, die der Wahrung des informationellen Selbstbestimmungsrechts durch einen angemessenen Interessensausgleich Rechnung trägt.

Die neue Regelung des Datenschutzaudits (§ 9 a) verfolgt das Ziel, datenschutzfreundliche Produkte auf dem Markt zu fördern, indem deren Datenschutzkonzept geprüft und bewertet wird.

Bereits bei der Novellierung des BDSG 1990 waren zuvor bestehende Unsicherheiten in der Rechtsanwendungspraxis hinsichtlich personenbezogener Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, durch Klarstellung im Rahmen der damaligen Neufassung von § 24 Abs. 1 und 2 beseitigt worden. Keine ausdrückliche Regelung bestand für die Kontrolle des Bundesbeauftragten für den Datenschutz hinsichtlich der von öffentlichen Stellen des Bundes erlangten personenbezogenen Daten über den Inhalt und die näheren Umstände des Brief-, Post- und Fernmeldeverkehrs. Vielmehr verwehrte § 24 Abs. 2 Satz 3 a.F., der den Inhalt des Post- und Fernmeldeverkehrs von der Kontrolle ausnahm, es dem Bundesbeauftragten für den Datenschutz, die Verwendung der durch Eingriffe in das Brief-, Post- und Fernmeldegeheimnis erlangten Daten zu kontrollieren. Dies soll mit der neuen Regelung des § 24 Abs. 2 ermöglicht werden.

Der neu eingefügte § 29 Abs. 3 beinhaltet eine Regelung, mit der folgendes erreicht wird: In den Fällen, in denen es sich bei Herausgebern elektronischer oder gedruckter Verzeichnisse nicht um Diensteanbieter im Sinne der Telekommunikationsdienstunternehmen-Datenschutzverordnung (TDSV) handelt, bestand bisher nur unzureichender Schutz der Betroffenen vor nicht gewollten Eintragungen in diese Verzeichnisse. Diese Regelungslücke schließt der neue § 29 Abs. 3.

2.4 Ausblick

Der vorliegende Gesetzentwurf sieht Änderungen des Bundesdatenschutzgesetzes überwiegend in dem Umfang vor, den die Richtlinie vorgibt. Noch in dieser Legislaturperiode soll eine umfassende Neukonzeption des BDSG vorbereitet werden, die das Gesetz modernisiert, vereinfacht und seine Lesbarkeit erhöht, sowie geprüft werden, inwieweit die in der Richtlinie für Zwecke der Forschung und der Statistik eingeräumten Spielräume genutzt werden sollen.

Ferner soll die Beratungs- und Servicefunktion der Datenschutzbeauftragten ausgebaut und gestärkt werden. Ziel dieser Neufassung ist die Verbesserung und Vereinheitlichung des Schutzes der Betroffenen im öffentlichen und im privaten Bereich.

Darüber hinaus wird das gesamte bereichsspezifische Datenschutzrecht daraufhin zu überprüfen sein, ob über die bereits vorgenommenen Änderungen hinaus weitere Anpassungen an die Richtlinie geboten sind, und zwar auch, soweit keine europarechtliche Anpassungspflicht besteht. Nur so kann vermieden werden, dass es auf Dauer zweierlei Datenschutzrecht mit unterschiedlich hohem Schutzniveau gibt.

In diesem Zusammenhang wird ein Arbeitnehmerdatenschutzgesetz und ein Informationszugangsgesetz zu kodifizieren sein.

Bisherige Fassung (a.F.)	**Neue Fassung (n.F.)**		***Begründung*[*)]**
		Inhaltsübersicht	*Die Inhaltsübersicht stand bei der Verabschiedung des Bundesdatenschutzgesetzes vor der Eingangsformel und nahm damit nicht am Gesetzesrang teil. Um dem Anwender die Übersicht und die Orientierung nicht nur für den Zeitpunkt des Inkrafttretens des Gesetzes, sondern für seine gesamte Geltungsdauer zu erleichtern, wird die Inhaltsübersicht in das Gesetz aufgenommen.*
		§ 1 Zweck und Anwendungsbereich des Gesetzes	
		§ 2 Öffentliche und nicht öffentliche Stellen	
		§ 3 Weitere Begriffsbestimmungen	***Die Änderung berücksichtigt die Neuaufnahme des § 6c sowie die Neufassung der §§ 43, 44.***
		§ 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	

[*)] Zur Herkunft des jeweiligen Begründungstextes siehe Formatierung: *Begründung RegE,* ***Begründung Ausschussempfehlung***

Erster Abschnitt **Allgemeine Bestimmungen**	**Erster Abschnitt** **Allgemeine und gemeinsame Bestimmungen**	
§ 1 a.F.	§ 1 n.F.	
Zweck und Anwendungsbereich des Gesetzes	Zweck und Anwendungsbereich des Gesetzes	
(1) Zweck dieses Gesetzes ist es, den einzelnen davor zu schützen, daß er durch den Umgang mit seinen personenbezoge-nen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.	(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	(2) Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch	
1. öffentliche Stellen des Bundes,	1. öffentliche Stellen des Bundes,	
2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landes-gesetz geregelt ist und soweit sie a) Bundesrecht ausführen oder b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt,	2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landes-gesetz 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 in oder aus Dateien geschäftsmäßig oder für berufliche oder gewerbliche Zwecke verarbeiten oder nutzen.	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	*Während der bisherige Absatz 2 Nr. 3 positiv die Tätigkeiten benannte, bei deren Vorliegen das Bundesdatenschutzgesetz zur Anwendung gelangte, schließt die Richtlinie in Artikel 3 Abs. 2 zweiter Spiegelstrich generell (zum Anwendungsbereich der Richtlinie, insbesondere zum Dateibegriff, vgl. die Begründung zu § 3) nur solche Datenverarbeitungen von ihrem Anwendungsbereich aus, die von einer „natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen werden“. Alle*

	denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.	*übrigen Datenverarbeitungen durch nicht-öffentliche Stellen werden daher – soweit es sich um automatisierte Verarbeitungen oder um (nicht-automatisierte) Dateien han-delt (vgl. hierzu die Begründung zu § 3 Abs. 2) – vom Anwendungsbereich der Richt-linie erfasst. Die Vorschrift des Absatzes 2 Nr. 3 war dementsprechend zu ändern.*
(3) Bei der Anwendung dieses Gesetzes gelten folgende Einschränkungen: 1. Für automatisierte Dateien, die ausschließlich aus verarbeitungstechnischen Gründen vorübergehend erstellt und nach ihrer verarbeitungstechni-schen Nutzung automatisch gelöscht werden, gelten nur die §§ 5 und 9. 2. Für nicht-automatisierte Dateien, deren personenbezogene Daten nicht zur Übermittlung an Dritte bestimmt sind, gelten nur die §§ 5, 9, 39 und 40. Außerdem gelten für Dateien öffentlicher Stellen die Regelungen über die Verarbeitung und Nutzung personenbezogener Daten in Akten. Werden im Einzelfall personenbezogene Daten übermittelt, gelten für diesen Einzelfall die Vorschriften dieses Gesetzes uneingeschränkt.	(3) [1]Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor. [2]Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.	*Absatz 3 war in Umsetzung von Artikel 3 Abs. 1 der Richtlinie aufzuheben, da die Richtlinie eine entsprechende Einschränkung des Anwendungsbereichs nicht vorsieht.*
(4) [1]Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor. [2]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) Die Vorschriften dieses Gesetzes gehen denen des Verwaltungsverfahrensge-	(5) [1]Dieses Gesetz findet keine Anwendung, sofern eine in einem anderen Mit-	*Artikel 4 der Richtlinie geht hinsichtlich des Anwendungsbereichs nationalen Daten-schutzrechts im grenzüberschreitenden Datenverkehr - anders als das derzeit geltende*

setzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.	gliedstaat 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. [2]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. [3]Soweit die verantwortliche Stelle nach diesem Gesetz zu nennen ist, sind auch Angaben über im Inland ansässige Vertreter zu machen. [4]Die Sätze 2 und 3 gelten nicht, sofern Datenträger nur zum Zwecke des Transits durch das Inland eingesetzt werden. [5]§ 38 Abs. 1 Satz 1 bleibt unberührt.	*Bundesdatenschutzgesetz - im Grundsatz nicht vom Territorialprinzip, sondern vom Sitzprinzip aus. Danach richtet sich das insoweit anzuwendende nationale Recht nicht nach dem Ort der Verarbeitung, sondern nach dem Sitz der verantwortlichen Stelle.* *Als Ausnahme hiervon gilt aber wieder das Territorialprinzip, wenn die verantwortliche Stelle aus einem Mitgliedstaat der Europäischen Union eine Niederlassung in einem anderen Mitgliedstaat der Europäischen Union unterhält. Für die Erhebung, Verarbei-tung oder Nutzung personenbezogener Daten durch diese Niederlassung gilt dann das nationale Datenschutzrecht des Landes, in dem sie belegen ist.* *Diese Regelung der Richtlinie stellt einen Kompromiss dar zwischen den Belangen der Wirtschaft einerseits: Diese soll ihr gewohntes nationales Datenschutzrecht "exportie-ren" dürfen und sich nicht durch unbekannte Datenschutzvorschriften in ihrer unternehmerischen Tätigkeit eingeschränkt sehen müssen. Andererseits wird dem Gesichtspunkt der Rechtssicherheit insbesondere im Zusammenhang mit den Schutzrechten der von derartigen Datenverarbeitungen Betroffenen Rechnung getragen. Dieser zweite Gesichtspunkt führte zur Ausnahmeregelung für Niederlassungen. Absatz 5 Satz 1 setzt daher insoweit Artikel 4 Abs. 1 Buchstabe a der Richtlinie um.* *Ausweislich des Erwägungsgrundes 19 der Richtlinie „setzt eine Niederlassung im Hoheitsgebiet eines Mitgliedstaats 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 maßgeb-lich." Zur Erläuterung des Begriffs Niederlassung kann auf die Definition der Niederlas-sung in § 42 Abs. 2 Gewerbeordnung verwiesen werden. Dieser zufolge ist eine Nie-derlassung vorhanden, wenn der Gewerbetreibende einen zum dauernden Gebrauch eingerichteten, ständig oder in regelmäßiger Wiederkehr von ihm benutzten Raum für den Betrieb seines Gewerbes besitzt.* *Zur Ersetzung des Begriffs „speichernde Stelle“ durch den Begriff der „verantwortlichen Stelle“ wird auf die Begründung zu § 3 Abs. 7 verwiesen.* *Artikel 4 Abs. 1 Buchstabe c der Richtlinie will – vom Grundsatz des Sitzprinzips ausgehend – verhindern, dass ein möglicherweise geringerer Datenschutzstandard als der in den Mitgliedstaaten der Europäischen Union vorhandene in den Fällen zur Geltung kommt, in denen Datenerhebungen, -verarbeitungen oder –nutzungen innerhalb der Europäischen Union durch außerhalb der Europäischen Union belegene speichernde Stellen vorgenommen werden. Die Richtlinie erklärt daher für diese Fälle - als Aus-nahme – das Territorialprinzip für anwendbar.* *Mit Blick auf das im Bundesdatenschutzgesetz im übrigen geltende Territorialprinzip ist der Artikel 4 Abs. 1 Buchstabe c der Richtlinie umsetzende Absatz 5 Satz 2 daher lediglich deklaratorisch. Er ist gleichwohl notwendig als Anknüpfungspunkt zum einen für die*

		Artikel 4 Abs. 2 der Richtlinie umsetzende Verpflichtung der speichernden Stelle zur Benennung eines Vertreters in diesen Fällen (Absatz 5 Satz 3). Zum anderen ist Absatz 5 Satz 2 erforderlich für die Umsetzung der aus deutscher Sicht ausnahmsweisen Geltung des Sitzprinzips in den Fällen, in denen Datenträger nur zum Zweck der Durchfuhr durch das Inland eingesetzt werden (Absatz 5 Satz 4). *Die Verpflichtung zur Benennung eines Vertreters will Transparenz in den Fällen sicherstellen, in denen die speichernde Stelle in einem Drittstaat belegen ist. Sowohl Betroffene als auch Aufsichtsbehörden sollen einen geeigneten Ansprechpartner haben, dem insoweit Mittlerfunktion zukommt.* *Absatz 5 Satz 4 findet Anwendung, wenn Übertragungswege benutzt werden, ohne dass von den personenbezogenen Daten Kenntnis genommen wird.* *Von einer Artikel 4 Abs. 1 Buchstabe b der Richtlinie umsetzenden Regelung konnte mit Blick auf die einschlägigen Regelungen des Völkerrechts abgesehen werden.* *Absatz 5 Satz 5 stellt klar, dass sich das Kontrollrecht der Aufsichtsbehörden auch auf die Fälle erstreckt, in denen aufgrund der Regelung des Absatzes 5 das Recht anderer Mitgliedstaaten der Europäischen Union zur Anwendung gelangt.* ***Die Änderung*** [Einbeziehung der EWR-Staaten] ***trägt der zum 1. Juli 2000 wirksam gewordenen Übernahme der Richtlinie durch die EWR-Staaten (dies sind die EU-Staaten sowie Norwegen, Island und Liechtenstein) Rechnung. Danach gilt das Gebot des freien Datenverkehrs (Artikel 1 Abs. 2 Richtlinie) auch im Verhältnis zwischen EU-Staaten und den übrigen EWR-Staaten. Norwegen und Island haben den Abschluss der Umsetzung der Richtlinie bereits notifiziert. Die Umsetzung der Richtlinie wird für die EWR-Staaten, die nicht zugleich Mitgliedstaaten der EU sind, gemeinsam von EG-Kommission und der Aufsichtsbehörde nach Artikel 108 EWR-Abkommen überwacht.***
§ 2 a.F.	§ 2 n.F.	
Öffentliche und nicht-öffentliche Stellen	Öffentliche und nicht-öffentliche Stellen	
(1) [1]Öffentliche Stellen des Bundes sind die Behörden, die Organe der Rechtspfle-ge und andere öffentlich-rechtlich organi-sierte Einrichtungen des Bundes, der bun-desunmittelbaren Körperschaften, Anstal-ten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform. [2]Als öffentliche Stellen gelten die aus dem Sondervermögen Deutsche	(1) [1]Öffentliche Stellen des Bundes sind die Behörden, die Organe der Rechtspfle-ge und andere öffentlich-rechtlich organi-sierte Einrichtungen des Bundes, der bun-desunmittelbaren Körperschaften, Anstal-ten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform. [2]Als öffentliche Stellen gelten die aus dem Sondervermögen Deutsche	

§ 3 a.F.	§ 3 n.F.
Bundespost durch Gesetz hervorgegangenen Unternehmen, solange ihnen ein ausschließliches Recht nach dem Postgesetz zusteht.	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 Ge-meinde, eines Gemeindeverbandes und sonstiger der Aufsicht des Landes unter-stehender juristischer Personen des öffent-lichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform.	(2) Öffentliche Stellen der Länder sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Landes, einer Ge-meinde, eines Gemeindeverbandes und sonstiger der Aufsicht des Landes unter-stehender juristischer Personen des öffent-lichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform.
(3) [1]Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder, die Aufgaben der öffentlichen Verwaltung wahrnehmen, gelten ungeach-tet der Beteiligung nicht-öffentlicher Stel-len als öffentliche Stellen des Bundes, wenn	(3) [1]Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder, die Aufgaben der öffentlichen Verwaltung wahrnehmen, gelten ungeach-tet der Beteiligung nicht öffentlicher Stel-len als öffentliche Stellen des Bundes, wenn
1. sie über den Bereich eines Landes hinaus tätig werden oder	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.	2. dem Bund die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht.
[2]Andernfalls gelten sie als öffentliche Stellen der Länder.	[2]Andernfalls gelten sie als öffentliche Stellen der Länder.
(4) [1]Nicht-öffentliche Stellen sind natürli-che und juristische Personen, Gesellschaf-ten und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Absätze 1 bis 3 fallen. [2]Nimmt eine nicht-öffentliche Stelle hoheitliche Aufga-ben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne die-ses Gesetzes.	(4) [1]Nicht öffentliche Stellen sind natürli-che und juristische Personen, Gesellschaf-ten und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Absätze 1 bis 3 fallen. [2]Nimmt eine nicht öffentliche Stelle hoheitliche Aufga-ben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne die-ses Gesetzes.

Weitere Begriffsbestimmungen	Weitere Begriffsbestimmungen	
(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).	(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).	
(2) [1]Eine Datei ist 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 aufge-baut ist und nach bestimmten Merkma-len geordnet, umgeordnet und ausge-wertet werden kann (nicht-automati-sierte Datei). [2]Nicht hierzu gehören Akten und Aktensammlungen, es sei denn, daß sie durch automatisierte Verfahren umgeordnet und ausgewertet werden können.	(2) [1]Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. [2]Eine nicht automatisierte Datei ist jede nicht automatisierte Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann.	*Während für das BDSG 1977 noch der Dateibezug für die Anwendbarkeit des Geset-zes maßgebend war, hat das BDSG 1990 grundsätzlich jedes Speichermedium einbe-zogen und lediglich im nicht-öffentlichen Bereich das Erfordernis des Dateibezugs bei-behalten (§ 1 Abs. 2 Nr. 3 a.F.).* *Die Richtlinie wiederum stellt – insofern vergleichbar dem BDSG 1977 – im Rahmen der Bestimmung des Anwendungsbereichs teilweise auf das Speichermedium „Datei“ ab. Kriterien für den sachlichen Anwendungsbereich des Bundesdatenschutzgesetzes sind nach Artikel 3 Abs. 1 der Richtlinie nunmehr die automatisierte Erhebung, Verar-beitung und Nutzung personenbezogener Daten sowie die nicht-automatisierte Erhe-bung, Verarbeitung und Nutzung personenbezogener Daten, die in einer Datei gespei-chert sind oder gespeichert werden sollen.* *Das Kriterium der Datei ist für die Frage der Eröffnung des sachlichen Anwendungsbereichs des Bundesdatenschutzgesetzes nur noch von Bedeutung, soweit es um die nicht-automatisierte Erhebung, Verarbeitung und Nutzung personenbezogener Daten geht. Diesem Ansatz folgt die Definition der nicht-automatisierten Datei in Satz 2. Fin-det hingegen eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten in einer automatisierten Datei statt, ist für die Anwendbarkeit des Bundesdatenschutzge-setzes nicht das Merkmal der automatisierten Datei von Relevanz, sondern nur und ausschließlich das der automatisierten Erhebung, Verarbeitung oder Nutzung.* *Dementsprechend war die Definition der automatisierten Datei in Absatz 2 Nr. 1a.F. in Satz 1 zu ersetzen durch eine Definition der automatisierten Verarbeitung.* *In Artikel 2 Buchstabe c definiert die Richtlinie „Datei“ als „jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind (...)“. Im Erwägungsgrund 27 der Richtlinie wird hierzu ausgeführt, dass „insbesondere der Inhalt einer Datei nach bestimmten personenbezogenen Kriterien strukturiert sein muss, 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.“ Der materielle Änderungsbedarf im Rahmen der Definition des Absatz 2 Satz 2 war daher beschränkt auf die Verdeutlichung des Merkmals „zugänglich“ durch dessen ausdrückliche Aufnahme in die*

		Definition anstelle der bisherigen Definitionsmerkmale „geordnet“ und „umgeordnet“, die der Zugänglichmachung dienen. *Auf die Regelung des Absatzes 2 Satz 2 a.F. konnte aus folgenden Gründen verzichtet werden: Hinsichtlich der Einbeziehung von Akten in den Anwendungsbereich des Bundesdatenschutzgesetzes neuer Fassung gilt grundsätzlich, dass diese immer dann der Richtlinie und somit auch dem Bundesdatenschutzgesetz unterfallen, wenn sie unter den Begriff der nicht-automatisierten Datei subsumierbar sind. Relevanz erlangt dies im nicht-öffentlichen Bereich, da hier Akten bisher weitgehend vom Anwendungsbereich ausgenommen waren. Maßgeblich ist insoweit Erwägungsgrund 27 der Richtlinie, dem-zufolge die Richtlinie „bei manuellen Verarbeitungen lediglich Dateien erfasst, nicht je-doch unstrukturierte Akten. (...) Akten und Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien strukturierbar sind, fallen unter keinen Umständen unter den Anwendungsbereich dieser Richtlinie.“ Anlässlich der Annahme der Richtlinie ist von Rat und Kommission folgende Erklärung unter Nr. 7 zu Protokoll gegeben wor-den: „Der Rat und die Kommission bestätigen, dass sich die Richtlinie nach der derzei-tigen Definition in Artikel 2 Buchstabe c nur auf Dateien erstreckt, nicht aber auf Akten; die Kriterien, nach denen sich die Bestandteile einer strukturierten Sammlung perso-nenbezogener Daten bestimmen lassen, sowie die Kriterien, nach denen diese Samm-lungen zugänglich sind,können von jedem einzelnen Mitgliedstaat festgelegt werden; Akten und Aktensammlungen und die Deckblätter dazu können nicht unter die unter dem ersten Gedankenstrich genannte Definition fallen, wenn ihr Inhalt nicht in der Art einer Datei strukturiert ist.“* *Absatz 2 Satz 2 war dementsprechend aufzuheben, da es für die Frage der Einbeziehung von Akten nicht mehr auf das Merkmal der automatisierten Auswertbarkeit ankommt. Ausschlaggebend ist anstelle dessen, ob eine nicht-automatisierte Datei vorliegt; eine manuelle Auswertbarkeit genügt insoweit.*
(3) [1]Eine Akte ist jede sonstige amtlichen oder dienstlichen Zwecken dienende Unterlage; dazu zählen auch Bild- und Tonträger. [2]Nicht hierunter fallen Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen.	(3) Erheben ist das Beschaffen von Daten über den Betroffenen.	*Der bislang in Absatz 4 geregelte Begriff des Erhebens findet sich nunmehr in Absatz 3. Da dem Begriff der Akte keine eigenständige Bedeutung mehr zukommt, war die Definition der Akte in Absatz 3 Satz 1 a.F. aufzuheben; hinsichtlich der Aufhebung von Absatz 3 Satz 1 zweiter Halbsatz a.F. gilt, dass nach Erwägungsgrund 14 der Richtlinie grundsätzlich personenbezogene Ton- und Bilddaten dem Anwendungsbereich der Richtlinie unterfallen. Erwägungsgrund 15 der Richtlinie führt hierzu aus, dass „die Verarbeitung solcher Daten von der Richtlinie nur erfasst wird, wenn sie automatisiert er-folgt 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 zu ermöglichen“. Maßgeblich für die Einbe-ziehung von Bild- und Tondaten ist daher die Möglichkeit der Subsumtion entweder unter den Begriff der automatisierten Verarbeitung im Sinne des Absatzes 2 Nr. 1 oder den der nicht-automatisierten Datei im Sinne des Absatzes 2 Nr. 2.*

(4) Erheben ist das Beschaffen von Daten über den Betroffenen.	(4) [1]Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. [2]Im einzelnen ist, ungeachtet der dabei angewendeten Verfahren: 1. Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung, 2. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten, 3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass a) die Daten an den Dritten weitergegeben werden oder b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft, 4. Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken, 5. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.	*Der Begriff der Übermittlung beinhaltet als notwendige Komponenten die Bekanntgabe, die speichernde Stelle als bekannt gebende Instanz sowie den Dritten im Sinne des Absatzes 8 als Adressaten. Der Begriff des Empfängers wurde in Absatz 5 Nr. 3 a.F. synonym neben dem des Dritten gebraucht. Eigenständige Bedeutung kam ihm nicht zu. Da in Umsetzung von Artikel 2 Buchstabe g der Richtlinie der weitergehende Begriff des Empfängers nunmehr in Absatz 8 Satz 1 definiert wird, war er in Absatz 4 Nr. 3 n.F. zur Vermeidung von Missverständnissen zu streichen bzw. durch den des Dritten zu ersetzen.*
(5) [1]Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. [2]Im einzelnen ist, ungeachtet der dabei angewendeten Verfahren: 1. Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwe-	(5) Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.	

cke 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 (Empfänger) in der Weise, daß a) die Daten durch die speichernde Stelle an den Empfänger weitergegeben werden oder b) der Empfänger von der speichern-den Stelle zur Einsicht oder zum Ab-ruf bereitgehaltene Daten einsieht oder abruft, 4. Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung ein-zuschränken, 5. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.		
(6) 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 Auf-wand an Zeit, Kosten und Arbeitskraft ei-ner bestimmten oder bestimmbaren natür-lichen 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.	*Neu aufzunehmen war eine Definition des Begriffs des Pseudonymisierens, da in § 3 a Satz 2 erstmals der vorrangige Einsatz (anonymer und) pseudonymer Formen der Datenverarbeitung vorgesehen ist.*

(7) Anonymisieren ist das Verändern personenbezogener Daten derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Auf-wand an Zeit, Kosten und Arbeitskraft ei-ner bestimmten oder bestimmbaren natür-lichen Person zugeordnet werden können.	(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.	*In Artikel 2 Buchstabe d Satz 1 der Richtlinie wird der Begriff des „für die Verarbeitung Verantwortlichen“ definiert als „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“. In Anpassung an diese Terminologie der Richtlinie wurde in Absatz 7 die Definition der speichernden Stelle durch die der verantwortlichen Stelle ersetzt.*
(8) Speichernde Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst speichert oder durch andere im Auftrag speichern läßt.	(8) [1]Empfänger ist jede Person oder Stelle, die Daten erhält. [2]Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. [3]Dritte sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.	*Absatz 8 Satz 1 setzt Artikel 2 Buchstabe g der Richtlinie um. Der Begriff des Empfängers ist sehr weit gefasst. Er umfasst neben dem Dritten, dem Betroffenen und denjenigen Personen und Stellen, die im Geltungsbereich des Bundesdatenschutzgesetzes personenbezogene Daten im Auftrag verarbeiten oder nutzen, auch die verschiedenen Organisationseinheiten innerhalb einer speichernden Stelle. Die negative Definition des Begriffs des Dritten in § 3 Abs. 9 Satz 2 a.F. war in Umsetzung von Artikel 1 Abs. 2 der Richtlinie um die Personen und Stellen zu erweitern, die im Geltungsbereich der Rechtsvorschriften zum Schutz personenbezogener Daten der Mitgliedstaaten der Europäischen Union personenbezogene Daten im Auftrag verarbeiten oder nutzen. Die Wörter „Geltungsbereich dieses Gesetzes“ wurden aus Gründen der Vereinheitlichung der Gesetzessprache nach Vollendung der Deutschen Einheit durch das Wort „Inland“ ersetzt.* ***Die Begründung zu § 1 Abs. 5 gilt entsprechend.***
(9) [1]Dritter ist jede Person oder Stelle außerhalb der speichernden Stelle. [2]Dritte sind nicht der Betroffene sowie diejenigen Personen und Stellen, die im Geltungsbereich dieses Gesetzes personenbezogene Daten im Auftrag verarbeiten oder nutzen.	(9) Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinun-gen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.	*Absatz 9 definiert die in Artikel 8 Abs. 1 der Richtlinie bezeichneten besonderen Kategorien personenbezogener Daten.*
	(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 Medi-	***Die neu aufgenommene Definition führt den in § 6c verwandten Begriff „mobile personenbezogene Speicher- und Verarbeitungsmedien“ ein. Erfasst werden ausschließlich Medien, auf denen personenbezogene Daten über die Speicherung hinaus automatisiert verarbeitet werden können (Nummer 2), die also mit einem Prozessorchip ausgestattet sind. Auch „blanko“ ausgegebene Medien, auf denen noch keine Verfahren oder personenbezogene Daten gespeichert sind, fal-len unter § 3 Abs. 10. In diesen Fällen ist der Begriff des „Betroffenen“ in einem weiteren Sinn zu verstehen als in § 3 Abs. 1 und umfasst auch den erst künftig Betroffenen.*** ***Bloße Speichermedien (CDs, Magnetkarten) werden nicht erfasst. Im Übrigen kommt es auf die Beschaffenheit und die Gestaltung des Mediums nicht an. Es muss keine Karte sein, sondern es kann sich auch um ein Armband, eine Halskette***

	ums beeinflussen kann.	***oder andere Gegenstände handeln.***
		Keine mobilen personenbezogenen Speicher- und Verarbeitungsmedien sind Mobiltelefone oder tragbare Personalcomputer, denn bei diesen Geräten kann der Benutzer die Verarbeitungsvorgänge auf vielfältige Weise steuern. Kennzeichnend für die mobilen personenbezogenen Speicher- und Verarbeitungsmedien ist hingegen, dass der Betroffene die Datenverarbeitung typischerweise nur dadurch beeinflussen kann, dass er das Medium, beispielsweise durch das Einführen in Lesegeräte, einsetzt. Der Begriff „Gebrauch“ erfasst darüber hinaus auch die Auswahl zwischen einigen wenigen vom Verfahren vorgegebenen Alternativen, etwa durch Drücken einer Taste am Lesegerät. Anders als durch Abruf der vom Verfahren bereit gestellten (objektorientierten) Routinen kann der Betroffene die Verarbeitung auch in diesen Fällen nicht steuern.
	§ 3 a n.F. Datenvermeidung und Datensparsamkeit	
	[1]Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. [2]Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.	*Der Grundsatz der Datenvermeidung und -sparsamkeit wird erstmalig in das allgemeine Datenschutzrecht aufgenommen. Die Vorschrift konkretisiert den Grundsatz der Verhältnismäßigkeit für die technische Gestaltung der Datenverarbeitungssysteme. Eine vergleichbare Regelung findet sich im bereichsspezifischen Teledienstedatenschutzgesetz in § 3 Abs. 4. Wie dort, soll durch die Einführung des Grundsatzes bereits durch die Gestaltung der Systemstrukturen die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten soweit wie möglich vermieden und dadurch Gefahren für das informationelle Selbstbestimmungsrecht des Betroffenen von vornherein minimiert wer-den. Dies bedeutet nicht, dass personenbezogene Daten, die für die Aufgabenerfüllung erforderlich sind, nicht erhoben, verarbeitet oder genutzt werden dürfen, wie z.B. beim Kraftfahrtbundesamt das Zentrale Verkehrsinformationssystem (ZEVIS), beim Bundesverwaltungsamt das Ausländerzentralregister (AZR), beim Bundeskriminalamt das polizeiliche Informationssystem (INPOL) sowie die bei den Nachrichtendiensten des Bun-des geführten Informationssysteme.* *Satz 2 beinhaltet den Vorrang anonymer und pseudonymer Formen der Datenverarbeitung als eine von mehreren Möglichkeiten der Ausgestaltung des Systemdatenschutzes als Mittel, dem Grundsatz der Erforderlichkeit Rechnung zu tragen. Hierbei geht es in erster Linie darum – soweit technisch möglich und aufgrund der vorgegebenen funktionalen Zusammenhänge sachgerecht – das Mitführen der vollen Identität Betroffener während der eigentlichen Datenverarbeitungsvorgänge zu reduzieren.*
§ 4 a.F. Zulässigkeit der Datenverarbeitung und	§ 4 n.F. Zulässigkeit der Datenerhebung, -verar-	

-nutzung	beitung und -nutzung	
(1) Die Verarbeitung personenbezogener Daten und deren Nutzung sind nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat.	(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.	*In Absatz 1 wurde der Begriff „Erhebung" aufgenommen, um den Anforderungen der Richtlinie insoweit Rechnung zu tragen, als auch die Erhebung personenbezogener Daten im privaten Sektor dem Vorbehalt des Gesetzes zu unterstellen ist. Dies folgt daraus, dass in Artikel 2 Buchstabe b der Richtlinie die Erhebung als Unterfall der Verarbeitung betrachtet und die Verarbeitung nach Artikel 7 nur zulässig ist, wenn der Betroffene eingewilligt hat oder die dort aufgeführten, in das nationale Recht zu übertragenden Voraussetzungen vorliegen. Die übrigen Änderungen des Absatzes 1 stellen sprachliche Präzisierungen dar.*
(2) [1]Wird die Einwilligung bei dem Betroffenen eingeholt, ist er auf den Zweck der Speicherung und einer vorgesehenen Übermittlung sowie auf Verlangen auf die Folgen der Verweigerung der Einwilligung hinzuweisen. [2]Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonde-rer Umstände eine andere Form angemes-sen ist. [3]Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben.	(2) [1]Personenbezogene Daten sind beim Betroffenen zu erheben. [2]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.	*Absatz 2 greift den Rechtsgedanken von § 13 Abs. 2 a.F. auf, erweitert ihn aber in Nummer 2 a für den nicht-öffentlichen Bereich.*
(3) [1]Im Bereich der wissenschaftlichen Forschung liegt ein besonderer Umstand im Sinne von Absatz 2 Satz 2 auch dann vor, wenn durch die Schriftform der be-stimmte Forschungszweck erheblich be-einträchtigt würde. [2]In diesem Fall sind der Hinweis nach Absatz 2 Satz 1 und die Gründe, aus denen sich die erhebliche Beeinträchtigung des bestimmten For-schungszweckes ergibt, schriftlich festzu-halten.	(3) [1]Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stel-le über 1. die Identität der verantwortlichen Stelle, 2. die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und 3. die Kategorien von Empfängern nur,	*Absatz 3 modifiziert § 13 Abs. 3 a.F. nach den Voraussetzungen des Artikels 10 der Richtlinie.* *Absatz 4 entspricht § 13 Abs. 4 a.F.* [Abs. 4 der Fassung des RegE wurde vom BT gestrichen] ***Mit der Streichung wird eine Prüfbitte des Bundesrates (BR-Drs. 461/00 – Beschluss, S. 3, Nr. 2, 1. Anstrich) aufgegriffen. Während eine Modifizierung der Regelung des § 4 Abs. 2 nicht geboten erscheint, kann die in § 4 Abs. 4 geregelte Hinweispflicht – entsprechend der bisherigen Gesetzesfassung – auf die Erhebung durch öffentliche Stellen beschränkt werden.*** [vgl. jetzt § 13 Abs. 1a]

soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss,

zu unterrichten. [2]Werden personenbezogene Daten beim Betroffenen aufgrund ei-ner 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. [3]Soweit nach den Umständen des Einzelfalles er-forderlich oder auf Verlangen, ist er über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären.

Durch die Hinweispflicht soll verhindert werden, dass eine nicht öffentliche Stel-le personenbezogene Daten übermittelt, obwohl sie hierzu von Rechts wegen nicht verpflichtet ist, sich aber irrtümlich für verpflichtet hält. Diese Gefahr besteht regelmäßig nur, wenn eine öffentliche Stelle das Übermittlungsersuchen – hoheitlich – stellt. Im Verhältnis zwischen Privaten ist dagegen nicht zu erwarten, dass einem Übermittlungsbegehren auch dann entsprochen wird, wenn es außerhalb einer – nicht eigens hinweisbedürftigen – vertraglichen Verpflichtung geltend gemacht wird.

§ 4 a n.F.

Einwilligung

(1) [1]Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. [2]Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. [3]Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. [4]Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie be-sonders hervorzuheben.

Absatz 1 Satz 1 berücksichtigt die Voraussetzungen des Artikels 2 Buchstabe h der Richtlinie, wonach die Einwilligung ohne Zwang erfolgen muss. Die Anfügung des Wor-tes „vorgesehenen“ vor dem Wort „Zweck“ in Satz 2 dient der sprachlichen Verdeutli-chung des Gewollten. Die Ersetzung der Wörter „Speicherung“ und „Übermittlung“ durch die Wörter „Erhebung, Verarbeitung und Nutzung“ dient der Vereinheitlichung des Sprachgebrauchs des Bundesdatenschutzgesetzes in Übereinstimmung mit der Termi-nologie der Richtlinie (vgl. hierzu auch die Begründung zu § 4). Die Einfügung der Wör-ter „soweit nach den Umständen des Einzelfalles erforderlich“ in Satz 2 dient der Um-setzung des Definitionsmerkmals „in Kenntnis der Sachlage“ nach Artikel 2 Buchsta-be h der Richtlinie. Die übrigen Anforderungen der Richtlinie sind bereits im Text des § 4 Abs. 2 a.F. verwirklicht, der im Folgenden wiedergegeben wird.

(2) [1]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. [2]In diesem Fall sind der Hinweis nach Absatz 1 Satz 2 und die Gründe, aus

Absatz 2 entspricht § 4 Abs. 3 a.F.

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.	*Absatz 3 sieht in Umsetzung des Artikels 8 Abs. 2 Buchstabe a der Richtlinie für die besonderen Arten personenbezogener Daten (§ 3 Abs. 9) besondere Voraussetzungen für die Wirksamkeit der Einwilligung für jene Daten vor.*
§ 4 b Übermittlung personenbezogener Daten ins Ausland sowie an über- oder zwischenstaatliche Stellen	
(1) Für die Übermittlung personenbezogener Daten an Stellen	*Die Vorschrift regelt - anders als § 17 BDSG a.F. - die Übermittlung personenbezoge-ner Daten ins Ausland sowohl für den öffentlichen als auch den nicht-öffentlichen Be-reich.*
1. in anderen Mitgliedstaaten der Europäischen Union,	*Absatz 1 beinhaltet eine Privilegierung für Übermittlungen öffentlicher und nicht-öffentlicher Stellen der Mitgliedstaaten der EU innerhalb des Anwendungsbereichs der ersten Säule des EU-Vertrags. Unabhängig von dieser Privilegierung kann die Übermittlung auch auf eine Einwilligung gestützt werden (§ 4 Abs. 1 a.E.).*
2. in anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum oder	***Die Änderung des § 4b*** [Einfügung der EWR-Staaten und EG-Organe und –Einrichtungen] ***trägt – in Entsprechung der Ergänzung des § 1 Abs. 5 – der zum 1. Juli 2000 wirksam gewordenen Übernahme der Richtlinie durch die EWR-Staaten Rechnung. Im Rahmen des § 4b ist auch die durch Artikel 286 EGV des Vertrages von Amsterdam wirksam gewordenen Geltung der Richtlinie für die Organe und Einrichtungen der Gemeinschaften, die für die Organe und Einrichtungen der Gemeinschaften durch das Europäische Parlament und den Rat in einer Datenschutzverordnung umgesetzt wurden, zu berücksichtigen.***
3. der Organe und Einrichtungen der Europäischen Gemeinschaften	
gelten § 15 Abs. 1, § 16 Abs. 1 und §§ 28 bis 30 nach Maßgabe der für diese Übermittlung geltenden Gesetze und Vereinbarungen, soweit die Übermittlung im Rahmen von Tätigkeiten erfolgt, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen.	***Bei Gelegenheit dieser Ergänzung empfiehlt sich zugleich eine redaktionelle Überarbeitung der ersten beiden Absätze der Vorschrift sowie des § 4c Abs. 1 und 2.***
(2) [1]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 zwischen-	*Absatz 2 findet Anwendung bei Übermittlungen an EU-Mitgliedstaaten außerhalb der ersten Säule des EU-Vertrags sowie an Drittstaaten. Absatz 2 Satz 2 ergänzt § 17 Abs. 1 a.F. um das Erfordernis des angemessenen Datenschutzniveaus im Drittstaat sowie bei über- und zwischenstaatlichen Stellen und genügt damit den Anforderungen des Artikels 25 Abs. 1 der Richtlinie. Damit wird die bislang in § 17 Abs. 2 a.F. enthaltene ordre-public-Klausel, die die Zulässigkeit grenzüberschreitender Übermittlungen von der Beachtung eines datenschutzrechtlichen Mindeststandards abhängig machte, über-*

staatliche Stellen gilt Absatz 1 entsprechend. [2]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 ange-messenes Datenschutzniveau nicht gewährleistet ist. [3]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.	*flüssig. Die Angemessenheit des Datenschutzniveaus in einem Drittstaat und das schutzwürdige Interesse des Betroffenen sind voneinander unabhängige Tatbestandsmerkmale. Um dem Gebot der Erforderlichkeit zu genügen, war für den öffentlichen Sektor die Bezugnahme auf § 15 Abs. 1 auszudehnen, § 16 Abs. 1 beizubehalten und die Regelungen der §§ 28 bis 30 für Datenübermittlungen nicht-öffentlicher Stellen zu ergänzen. Satz 3 beinhaltet Ausnahmen von Satz 2 für öffentliche Stellen des Bundes.* *Ferner bestimmt die Vorschrift entsprechend Artikel 25 Abs. 1 der Richtlinie, dass im Fall einzelstaatlicher Bestimmungen zur Regelung der Übermittlung personenbezoge-ner Daten in Drittstaaten, die mit der Richtlinie vereinbar sind, die Vorschriften der §§ 16 Abs. 1 und 28 bis 30 nach Maßgabe dieser Gesetze anzuwenden sind. Entspre-chendes gilt für völkerrechtliche Verträge, die im Hinblick auf Voraussetzungen und/ oder Umfang der Datenübermittlungen nicht erschöpfend sind und für Vereinbarungen mit zwischen- und überstaatlichen Stellen.*
(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 be-treffenden Empfänger geltenden Rechts-normen sowie die für ihn geltenden Standesregeln und Sicherheitsmaßnahmen herangezogen werden.	*Absatz 3 beinhaltet dem Artikel 25 Abs. 2 der Richtlinie entnommene Kriterien zur Bestimmung des angemessenen Datenschutzniveaus.*
(4) [1]In den Fällen des § 16 Abs. 1 Nr. 2 unterrichtet die übermittelnde Stelle den Betroffenen von der Übermittlung seiner Daten. [2]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.	*Absatz 4 übernimmt die Regelung des § 17 Abs. 1, letzter Halbsatz a.F., wonach der Betroffene bei Übermittlungen nach Maßgabe des § 16 Abs. 1 Nr. 2 zu unterrichten ist. Es bestand kein Anlass, diese Regelung auf andere Fallgruppen der Übermittlung personenbezogener Daten in Drittstaaten auszudehnen, da die Richtlinie keine entsprechende Vorschrift enthält. Insofern verbleibt es bei der Anwendung der Regelung des § 19 a, der Artikel 11 der Richtlinie umsetzt.*
(5) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde	*Absatz 5 entspricht § 17 Abs. 3 a.F.*

Stelle.	
(6) Die Stelle, an die die Daten übermittelt werden, ist auf den Zweck hinzuweisen, zu dessen Erfüllung die Daten übermittelt werden.	*Absatz 6 entspricht § 17 Abs. 4 a.F.* [Abs. 6 der Fassung des RegE wurde durch BT-Beschluss vom 06.04.2001 in die nebenstehende Fassung abgeändert.] ***Durch die Änderung des § 4b Absatz 6 wird die dort enthaltene Hinweispflicht auf die Mitteilung des Übermittlungszwecks beschränkt. Die Mitteilung dient der Beachtung des Zweckbindungsgebots nach Artikel 6 Abs. 1b der Richtlinie durch die Stelle, der die Daten übermittelt werden. Da das Zweckbindungsgebot nach der Richtlinie nicht uneingeschränkt gilt, kann der Hinweis in deren Geltungsbereich keine weitergehende Wirkung entfalten.***
§ 4 c Ausnahmen	
(1) [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	*Diese Vorschrift beinhaltet Erleichterungen für die Übermittlung personenbezogener Daten an Drittstaaten sowie an über- und zwischenstaatliche Stellen innerhalb des Anwendungsbereichs der ersten Säule des EU-Vertrags. Keine Anwendung findet die Vorschrift auf Übermittlungen von Stellen außerhalb der ersten Säule des EU-Vertrags: Insoweit gelangt § 4 b Abs. 2 ff. zur Anwendung.*
1. der Betroffene seine Einwilligung gegeben hat,	*Die Regelung des Absatzes 1 ergänzt die strikte Regelung des § 4 b Abs. 2 durch ei-nen weitreichenden Ausnahmekatalog. Diese in Anlehnung an Artikel 26 der Richtlinie formulierten Ausnahmen sollen dafür Sorge tragen, dass der Wirtschaftsverkehr mit Drittstaaten nicht unangemessen beeinträchtigt wird. Die Ausnahmen basieren auf dem Grundgedanken, dass das Schutzbedürfnis des Betroffenen geringer ist, wenn er über die Tatsache der Notwendigkeit der Übermittlung seiner Daten in einen Drittstaat infor-miert ist. Dass die in Nr. 1 entsprechend Artikel 26 Abs. 1 Buchstabe a der Richtlinie nochmals aufgenommene Einwilligung eine Übermittlung zulässt, ergibt sich bereits aus § 4 Abs. 1 a.F. (vgl. auch die Begründung zu § 4 b Abs. 1). Ferner soll der Schutz des Persönlichkeitsrechts zurücktreten, wenn ein wichtiges öffentliches Interesse, die Ver-teidigung von Rechtsansprüchen vor Gericht oder der für öffentliche Register geltende Publizitätsgrundsatz es erfordern. Hier, wie auch im Fall der Unfähigkeit des Betroffe-nen seinen Willen zu bekunden (vgl. Nummer 5), ist Maßstab für die Frage der Zuläs-sigkeit und des Umfangs der Übermittlung der Grundsatz der Verhältnismäßigkeit, der eine Abwägung der widerstreitenden Interessen gebietet. Die Regelung des Absatzes 1 gilt entsprechend dem Grundsatz von § 1 Abs. 4 nicht, wenn einer Übermittlung perso-nenbezogener Daten spezielle Verwendungsbeschränkungen entgegenstehen. In die-sem Fall kann trotz Vorliegens der Voraussetzungen des Absatzes 1 von einer Über-mittlung in den Drittstaat abgesehen werden. Dieser Gedanke findet seinen Nieder-schlag in Artikel 26 Abs. 1 der Richtlinie und in Nummer 60 der Erwägungsgründe. Satz 2 entspricht § 17 Abs. 4 a.F.*
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.

[2]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) [1]Unbeschadet des Absatzes 1 Satz 1 kann die zuständige Aufsichtsbehörde einzelne Übermittlungen oder bestimmte Ar-ten 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. [2]Bei den Post- und Telekommunikationsunternehmen ist der Bundesbeauftragte für den Datenschutz zuständig. [3]Sofern die Übermitt-

Nach Absatz 2 können die Aufsichtsbehörden der Länder Ausnahmen erteilen, die über den Katalog des Absatzes 1 hinausgehen. Kommt die verantwortliche Stelle zu dem Ergebnis, dass ein angemessenes Datenschutzniveau im Drittstaat nicht vorhanden ist, kann sie ein angemessenes Schutzniveau auch auf andere Weise garantieren. Geeignete Garantien in diesem Sinne können sich insbesondere aus Vertragsklauseln oder verbindlichen Unternehmensregelungen ergeben. Die Einbeziehung verbindlicher Unternehmensregelungen trägt der Tatsache Rechnung, dass sich die Problematik der Übermittlung personenbezogener Daten auch in internationalen Unternehmen stellt, wenn einzelne ihrer Teilunternehmen in Ländern ohne angemessenes Datenschutz-niveau angesiedelt sind. Das Verhältnis der Teilunternehmen untereinander ist nicht zwingend durch Vertragsklauseln geprägt. Internationale Konzerne gehen vielmehr ver-mehrt dazu über, für alle Teilunternehmen unabhängig von ihrem Standort verbindliche Regelungen über den Datenschutz zu erlassen („codes of conduct"). Sowohl Vertrags-klauseln als auch verbindliche Unternehmensregelungen sind der Aufsichtsbehörde zur Genehmigung vorzulegen. Im öffentlichen Bereich stellen die verantwortlichen Stellen selbst das Vorliegen ausreichender Garantien im Sinne des Satzes 1 sicher.

lung 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.	*Absatz 3 setzt Artikel 26 Abs. 3 der Richtlinie um. Die in der Richtlinie darüber hinaus vorgesehene Unterrichtungsverpflichtung der Mitgliedstaaten gegenüber der Kommis-sion sowie untereinander bedurfte keiner Umsetzung in nationales Recht.*
§ 4 d n.F. Meldepflicht	
(1) Verfahren automatisierter Verarbeitungen sind vor ihrer Inbetriebnahme von nicht öffentlichen verantwortlichen Stellen der zuständigen Aufsichtsbehörde und von öffentlichen verantwortlichen Stellen des Bundes sowie von den Post- und Telekommunikationsunternehmen dem Bundesbeauftragten für den Datenschutz nach Maßgabe von § 4e zu melden.	*§ 4 d in Verbindung mit § 4 e regelt die Meldepflicht für automatisierte Verarbeitungen öffentlicher und nicht-öffentlicher Stellen. Die Regelungen ersetzen § 26 Abs. 5 Satz 3 und § 32 a.F.* *Absatz 1 beinhaltet den Grundsatz der Meldepflicht automatisierter Verarbeitungen.* ***Der Bundesrat hat um Prüfung gebeten, ob in § 4d klargestellt werden kann, dass sich die in dieser Vorschrift begründete Meldepflicht nicht auf jeden einzelnen Verarbeitungsvorgang bezieht, sondern auf den Einsatz eines automatisierten Verfahrens als Ganzes (BR-Drs. 461/00 – Beschluss, S. 3, Nr. 2, 2. Anstrich). Die erbetene Klarstellung verstößt nicht gegen Artikel 18 Abs. 1 der Richtlinie, da dort Meldepflichten für den einzelnen Verarbeitungsvorgang nicht begründet werden. Der Begriff „Verfahren automatisierter Verarbeitungen“ trägt dem Anliegen des Bundesrates Rechnung. Die Änderung ist dementsprechend auch im Einleitungssatz des § 4e vorzunehmen.***
(2) Die Meldepflicht entfällt, wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt hat.	*Die Absätze 2 und 3 beinhalten Ausnahmen von der Meldepflicht.* *Absatz 2 setzt Artikel 18 Abs. 2, 2. Spiegelstrich der Richtlinie um. Damit kann die Meldepflicht im öffentlichen Bereich vollständig entfallen, da dort die Bestellung eines behördlichen Beauftragten für den Datenschutz obligatorisch ist. Dies gilt trotz der in Absatz 4 geregelten Rückausnahme, da Absatz 4 nur im nicht-öffentlichen Bereich Anwendung findet (vgl. insoweit die Begründung zu Absatz 4). Die Meldepflicht entfällt auch dann, wenn unbeschadet einer Verpflichtung zur Bestellung eines Beauftragten für Datenschutz dieser freiwillig bestellt wird.*
(3) Die Meldepflicht entfällt ferner, wenn die verantwortliche Stelle personenbezogene Daten für eigene Zwecke erhebt, ver-arbeitet oder nutzt, hierbei höchstens vier Arbeitnehmer mit der Erhebung, Verarbei-tung oder Nutzung personenbezogener Daten beschäftigt und entweder eine Einwilligung der Betroffenen vorliegt oder die Erhebung,	*Absatz 3 setzt Artikel 18 Abs. 2, 1. Spiegelstrich der Richtlinie um. Hiernach kann die Meldepflicht entfallen, wenn für Verarbeitungskategorien, bei denen unter Berücksichtigung der zu verarbeitenden Daten eine Beeinträchtigung der Rechte und Freiheiten der betroffenen Person unwahrscheinlich ist, die Zweckbestimmung der Verarbeitung, die Daten oder Kategorien der verarbeiteten Daten, die Kategorien der betroffenen Per-sonen, die Empfänger oder Kategorien der Empfänger, denen die Daten weitergegeben werden und die Dauer der Aufbewahrung festgelegt werden. Da die Bestellung eines Beauftragten für den Datenschutz nach § 4 f Abs. 1 Satz 1 im öffentlichen Bereich ob-ligatorisch ist,*

Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit den Betroffenen dient.	*die Meldepflicht im öffentlichen Bereich somit bereits nach Absatz 2 ent-fällt, ist für die Anwendung von Absatz 3 im öffentlichen Bereich kein Raum.* *Verarbeitungskategorie im Sinne dieser Vorschrift ist die Verarbeitung für eigene Zwecke. Anwendungsbeispiele für den Ausnahmetatbestand des Absatzes 3 sind Datenverarbeitungen,wie sie typischerweise bei einer Reihe von selbständig Berufstätigen, etwa Architekten, Ärzten, Apothekern, Handwerkern, Sanitätshäusern, Optikern, Fitnessstudios und kleinen Gewerbetreibenden und für die Verarbeitung des Merkmals „Religionszugehörigkeit“ durch den Arbeitgeber zwecks Abführung der Kirchensteuer in Betracht kommen. Dies gilt auch, soweit Daten nach § 3 Abs. 9 verarbeitet werden.*
(4) Die Absätze 2 und 3 gelten nicht, wenn es sich um automatisierte Verarbeitungen handelt, in denen geschäftsmäßig personenbezogene Daten von der jeweiligen Stelle 1. zum Zweck der Übermittlung oder 2. zum Zweck der anonymisierten Übermittlung gespeichert werden.	*Absatz 4 ist die Rückausnahme der Absätze 2 und 3. Absatz 4 findet ausweislich seines Wortlauts ("geschäftsmäßig") nur im nicht-öffentlichen Bereich Anwendung, die Nummern 1 und 2 entsprechen § 32 Abs. 1 Nr. 1 und 2 a.F.*
(5) [1]Soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, unterliegen sie der Prüfung vor Beginn der Verarbeitung (Vorabkontrolle). [2]Eine Vorabkontrolle ist insbesondere durchzuführen, wenn 1. besondere Arten personenbezogener Daten (§ 3 Abs. 9) verarbeitet werden oder 2. die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens, es sei denn, dass eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung der Zweckbestim-	*Absatz 5 bestimmt in Umsetzung von Artikel 20 Abs. 1 der Richtlinie die automatisierten Verarbeitungen, die der Vorabkontrolle unterliegen. Erwägungsgrund 53 der Richt-linie führt hierzu aus: „Bestimmte Verarbeitungen können jedoch aufgrund ihrer Art, ih-rer 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.“ Erwägungsgrund 54 der Richtlinie ergänzt: „Bei allen in der Gesellschaft durchgeführten Verarbeitungen sollte die Zahl der Verarbeitungen mit solchen besonderen Risiken sehr beschränkt sein.“ Die dem § 4 d unterfallenden automatisierten Verarbeitungen unterliegen der Vorabkontrolle aber nicht uneingeschränkt, sondern nur insoweit, als sie tatsächlich besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen.* *Im Gegensatz zur bloßen Meldepflicht stellt die Vorabkontrolle ein Verfahren zur Prüfung der materiellen Zulässigkeit der Datenverarbeitung dar.* *Grundlage der insoweit vorzunehmenden Prüfung sind die Angaben nach § 4 e, insbesondere der Nummern 5, 6 und 9.* *In Anlehnung an Art. 28 Abs. 1 des Vorschlags einer Verordnung des Europäischen Par-*

mung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient.	*laments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr vom 01. Oktober 1999 (BR-Drs.: 546 /99) werden in Satz 2 die Verarbeitung der in § 3 Abs. 9 genannten Datenarten sowie Verarbeitungen, die dazu bestimmt sind, die Persönlichkeit der betroffenen Person zu bewerten einschließ-lich ihrer Fähigkeiten, ihrer Leistung oder ihres Verhaltens, als Fälle aufgeführt, in de-nen eine Vorabkontrolle regelmäßig durchzuführen ist. Um eine sachgerechte Eingren-zung der Fälle der Vorabkontrolle zu erreichen, gilt dies nicht, wenn der Datenverarbei-tung eine gesetzliche Verpflichtung oder eine Einwilligung zugrunde liegt oder diese der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensver-hältnisses mit dem Betroffenen dient.*
(6) [1]Zuständig für die Vorabkontrolle ist der Beauftragte für den Datenschutz. [2]Die-ser nimmt die Vorabkontrolle nach Empfang der Übersicht nach § 4g Abs. 2 Satz 1 vor. [3]Er hat sich in Zweifelsfällen an die Aufsichts-behörde oder bei den Post- und Telekom-munikationsunternehmen an den Bundes-beauftragten für den Datenschutz zu wen-den.	*Absatz 6 setzt Artikel 20 Abs. 2 der Richtlinie um. Absatz 6 Satz 1 bestimmt den Beauftragten für den Datenschutz als zuständig für die Vorabkontrolle. Die Regelung der Verfahrensweise des Beauftragten für den Datenschutz entspricht der in § 4 g Abs. 1 Satz 2. Im Gegensatz zu dieser Regelung verpflichtet Satz 3 – der auf Artikel 20 Abs. 2 zweite Alternative der Richtlinie beruht – aber den Beauftragten für den Datenschutz zur Einbindung der Aufsichtsbehörde. In diesem Fall gibt die Aufsichtsbehörde im Rah-men ihrer Befugnisse nach § 38 als Ergebnis ihrer Überprüfung eine Stellungnahme ab.*
§ 4 e n.F. Inhalt der Meldepflicht	
[1]Sofern Verfahren automatisierter Verarbeitungen meldepflichtig sind, sind folgende Angaben zu machen:	
1. Name oder Firma der verantwortlichen Stelle,	*Der Katalog des § 4 e entspricht in den Nummern 1 bis 3 dem § 32 Abs. 2 Nr. 1 bis 3 a.F. Gleichzeitig wird hierdurch Artikel 19 Abs. 1 Buchstabe a der Richtlinie umgesetzt.*
2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Daten-verarbeitung beauftragten Personen,	
3. Anschrift der verantwortlichen Stelle,	
4. Zweckbestimmungen der Datenerhe-bung, -verarbeitung oder -nutzung,	*Nummer 4 setzt Artikel 19 Abs. 1 Buchstabe b der Richtlinie um und entspricht § 18 Abs. 2 Nr. 2 a.F. sowie § 32 Abs. 2 Nr. 4 a.F.*
5. eine Beschreibung der betroffenen Per-	*Nummer 5 setzt Artikel 19 Abs. 1 Buchstabe c der Richtlinie um und entspricht in sei-*

sonengruppen und der diesbezüglichen Daten oder Datenkategorien,	*nem ersten Teil § 18 Abs. 2 Nr. 4 a.F. Dabei soll insbesondere ersichtlich sein, ob es sich um Daten nach § 3 Abs. 9 handelt.*
6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,	*Nummer 6 setzt Artikel 19 Abs. 1 Buchstabe d der Richtlinie um und entspricht dem zweiten Teil von § 18 Abs. 2 Nr. 5 a.F. sowie dem ersten Teil von § 32 Abs. 3 Nr. 2 a.F.*
7. Regelfristen für die Löschung der Daten,	*Nummer 7 entspricht § 18 Abs. 2 Nr. 6 a.F.*
8. eine geplante Datenübermittlung in Drittstaaten,	*Durch Nummer 8 wird Artikel 19 Abs. 1 Buchstabe e der Richtlinie umgesetzt.*
9. eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.	*Nummer 9 verwirklicht die Voraussetzungen von Artikel 19 Abs. 1 Buchstabe f der Richtlinie.*
[2]§ 4d Abs. 1 und 4 gilt für die Änderung der nach Satz 1 mitgeteilten Angaben so-wie für den Zeitpunkt der Aufnahme und der Beendigung der meldepflichtigen Tätigkeit entsprechend.	*Satz 2, der der bisherigen Regelung in § 32 Abs. 4 a.F. entspricht, setzt Artikel 19 Abs. 2 der Richtlinie um. Darüber hinaus erstreckt er die Meldepflicht auch auf den Zeitpunkt der Aufnahme und der Beendigung der meldepflichtigen Tätigkeit.*
§ 4 f n.F. Beauftragter für den Datenschutz	
(1) [1]Öffentliche und nicht öffentliche Stellen, die personenbezogene Daten automa-tisiert erheben, verarbeiten oder nutzen, haben einen Beauftragten für den Datenschutz schriftlich zu bestellen. [2]Nicht öffentliche Stellen sind hierzu spätestens innerhalb eines Monats nach Aufnahme ihrer Tätigkeit verpflichtet. [3]Das Gleiche gilt, wenn personenbezogene Daten auf andere Weise erhoben, verarbeitet oder genutzt werden und damit in der Regel mindestens 20 Personen beschäftigt sind. [4]Die Sätze 1 und 2 gelten nicht für nicht öffentliche Stellen, die höchstens vier Arbeitnehmer mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigen. [5]Soweit aufgrund	*Die Regelungen des § 4 f gelten sowohl für die betrieblichen als auch für die behördlichen Beauftragten für den Datenschutz.* *Absatz 1 Satz 1 führt den behördlichen Beauftragten für den Datenschutz als obligatorische Institution ein. Satz 2 entspricht der Regelung des § 36 Abs. 1 Satz 1 a.F. Satz 3 entspricht der Regelung des § 36 Abs. 1 Satz 2 a.F. Satz 4 begrenzt die Verpflichtung zur Einführung eines betrieblichen Beauftragten für den Datenschutz bei automatisier-ten Datenverarbeitungen in Anlehnung an § 36 Abs. 1 Satz 1 a.F. Die in Satz 5 vorge-sehene bereichsübergreifende Bestellung eines Beauftragten für den Datenschutz im öffentlichen Bereich betrifft beispielsweise die Behörden des Bundesgrenzschutzes und des Bundesministeriums der Verteidigung. So kann etwa bei den Behörden des Bundesgrenzschutzes die Bestellung eines Beauftragten für den Datenschutz in einer Mittelbehörde ausreichend sein, um auch die Aufgabenbereiche der nachgeordneten Behörden mit zu betreuen. Im Geschäftsbereich des Bundesministeriums der Verteidigung werden auch die Aufgaben zur Überwachung der Ausführung dieses Gesetzes in der bestehenden Regelorganisation der Streitkräfte und der Wehrverwaltung wahrgenom-men. Diese Organisationsform bleibt durch die zu bestellenden Beauftragten für den Daten-*

der Struktur einer öffentlichen Stelle erforderlich, genügt die Bestellung eines Beauftragten für den Datenschutz für mehrere Bereiche. [6]Soweit nicht öffentliche Stellen automatisierte Verarbeitungen vornehmen, die einer Vorabkontrolle unterliegen oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung oder der anonymisierten Übermittlung erheben, verarbeiten oder nutzen, haben sie unabhängig von der Anzahl der Arbeitnehmer einen Beauftragten für den Datenschutz zu be-stellen.	*schutz unberührt. Sie werden entsprechend Satz 5 für mehrere Bereiche bestellt und sind auf Zusammenarbeit mit den Aufgabenträgern der Regelorganisation ange-wiesen. Nur so kann der unvermeidliche zusätzliche Personalaufwand in Grenzen ge-halten werden. Die Regelung des Satzes 6 betrifft nur den nicht-öffentlichen Bereich: Nach § 4 d Abs. 4 sind unter anderem Auskunfteien und Adresshandelsunternehmen sowie Markt- und Meinungsforschungsinstitute verpflichtet, die Aufnahme ihrer Tätigkeit der zuständigen Aufsichtsbehörde mitzuteilen. Damit sollen die Kontrollstellen in die Lage versetzt werden, frühzeitig den besonderen Risiken begegnen zu können, die mit der Erhebung, Nutzung und Verarbeitung personenbezogener Daten durch die vorge-nannten Stellen verbunden sind. Aus den gleichen Gründen ist es sachgerecht, für Stellen, die regelmäßig eine Vielzahl personenbezogener Daten zum Zwecke der Über-mittlung oder der anonymisierten Übermittlung erheben und speichern, unabhängig von der Anzahl der Mitarbeiter eine Verpflichtung zur Bestellung eines betrieblichen Beauf-tragten für den Datenschutz vorzusehen.* ***Die Änderung*** [des Satzes 6: Ersetzung von „eine Vorabkontrolle durchzuführen haben“ durch „automatische Verarbeitungen vornehmen, die einer Vorabkontrolle unterliegen“] ***beruht auf einem Vorschlag des Bundesrates (BR-Drs. 461/00 – Beschluss, S. 5, Nr. 4). Sie stellt klar, dass die Verpflichtung zur Bestellung eines Beauftragten für den Datenschutz nicht auf die Durchführung einer Vorabkon-trolle beschränkt ist, sondern für die gesamte Dauer der Verarbeitung personenbezogener Daten, für die eine Vorabkontrolle durchzuführen ist, besteht.***
(2) [1]Zum Beauftragten für den Datenschutz darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. [2]Mit dieser Aufgabe kann auch eine Person außerhalb der verantwortlichen Stelle betraut werden. [3]Öffentliche Stellen können mit Zustimmung ihrer Aufsichtsbehörde einen Bediensteten aus einer anderen öffentlichen Stelle zum Beauftragten für den Datenschutz bestellen.	*Absatz 2 Satz 1 entspricht § 36 Abs. 2 a.F. Satz 2 sieht die Möglichkeit vor, sich anstelle eines internen Beauftragten für den Datenschutz der Dienste eines externen Beauftragten für den Datenschutz zu bedienen. Satz 3 sieht dies unter den dort genannten Voraussetzungen für öffentliche Stellen vor.*
(3) [1]Der Beauftragte für den Datenschutz ist dem Leiter der öffentlichen oder nicht öffentlichen Stelle unmittelbar zu unterstel-len. [2]Er ist in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. [3]Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. [4]Die	*Absatz 3 entspricht § 36 Abs. 3 a.F., gilt nun aber auch für den behördlichen Beauftragten für den Datenschutz. Leiter im Sinne des Absatzes 3 Satz 1 umfasst als Oberbegriff sowohl die in § 36 Abs. 3 Satz 1 a.F. aufgezählten Funktionen als auch Leiter von Behörden. Absatz 3 Satz 2 entspricht § 36 Abs. 3 Satz 2 a.F. Dies verdeutlicht, dass die Weisungsfreiheit nicht absolut, sondern funktionsbezogen ausgestaltet ist, um die unabhängige Beratung des Leiters zu gewährleisten. Der Erteilung von gezielten Prüfaufträgen durch den Leiter steht die Weisungsfreiheit ebenso wenig entgegen wie der Wahrneh-*

Bestellung zum Beauftragten für den Datenschutz kann in entsprechender Anwendung von § 626 des Bürgerlichen Gesetzbuches, bei nicht öffentlichen Stellen auch auf Verlangen der Aufsichtsbehörde, widerrufen werden.	*mung der Dienstaufsicht. Absatz 3 Satz 3 entspricht § 36 Abs. 3 Satz 3 a.F. Die Regelung in Absatz 3 Satz 4 entspricht § 36 Abs. 3 Satz 4 a.F. und gilt partiell nunmehr auch für öffentliche Stellen.*
(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.	*Absatz 4 entspricht § 36 Abs. 4 a.F.*
(5) [1]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. [2]Betroffene können sich jederzeit an den Beauftragten für den Datenschutz wenden.	*Absatz 5 erweitert den Anwendungsbereich der Vorschrift auf die öffentlichen Stellen, entspricht im Übrigen aber in Satz 1 § 36 Abs. 5 a.F. Satz 2 beinhaltet ein Anrufungsrecht des Betroffenen gegenüber dem Beauftragten für den Datenschutz, vergleichbar der Anrufung des Bundesbeauftragten für den Datenschutz nach § 21.*
§ 4 g n.F. Aufgaben des Beauftragten für den Datenschutz	
(1) [1]Der Beauftragte für den Datenschutz wirkt auf die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz hin. [2]Zu diesem Zweck kann sich der Beauftragte für den Datenschutz in Zweifelsfällen an die für die Datenschutzkontrolle bei der verantwortlichen Stelle zuständige Behörde wenden. [3]Er hat insbesondere	*Absatz 1 entspricht im wesentlichen § 37 Abs. 1 a.F. Der Begriff „hinzuwirken“ wird der Aufgabe der betrieblichen und auch behördlichen Beauftragten für den Datenschutz am Besten gerecht. Satz 2 bezieht als Konsequenz des obligatorischen behördlichen Beauftragten für den Datenschutz den Bundesbeauftragten für den Datenschutz in die Regelung ein, setzt aber insoweit das Benehmen mit dem Leiter der verantwortlichen Stel-le voraus. Satz 3 beinhaltet eine Regelung zur Beilegung von Unstimmigkeiten zwi-schen dem behördlichen Beauftragten für den Datenschutz und dem Leiter der verant-wortlichen Stelle. Satz 4 Nr. 2 enthält eine sprachliche Straffung ohne inhaltliche Aus-wirkung.*
1. die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten ver-	

	arbeitet 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) [1]Dem Beauftragten für den Datenschutz ist von der verantwortlichen Stelle eine Übersicht über die in § 4e Satz 1 ge-nannten Angaben sowie über zugriffsberechtigte Personen zur Verfügung zu stellen. [2]Im Fall des § 4d Abs. 2 macht der Beauftragte für den Datenschutz die Anga-ben nach § 4e Satz 1 Nr. 1 bis 8 auf Antrag jedermann in geeigneter Weise verfügbar. [3]Im Fall des § 4d Abs. 3 gilt Satz 2 entsprechend für die verantwortliche Stelle.	*Absatz 2 Satz 1 setzt unter Einbeziehung des § 18 Abs. 2 Nr. 7 a.F. Artikel 18 Abs. 2, 2. Spiegelstrich, 2. Unterstrich der Richtlinie um. Absatz 2 Satz 2 setzt Artikel 21 Abs. 3 der Richtlinie für die Fälle um, in denen ein Beauftragter für den Datenschutz vorhan-den ist. Absatz 2 Satz 3 setzt Artikel 21 Abs. 3 der Richtlinie in den Fällen des § 4 f Abs. 1 Satz 4 in Verbindung mit § 4 d Abs. 3 um, findet also Anwendung, wenn eine nicht-öffentliche Stelle aufgrund von § 4 f Abs. 1 Satz 4 keinen Beauftragten für den Daten-schutz bestellt hat und auch nicht meldepflichtig nach § 4 d Abs. 3 ist. Die Ver-pflichtung des Beauftragten für den Datenschutz, die Angaben auf Antrag jedermann in geeigneter Weise verfügbar zu machen, ist bei den in § 6 Abs. 2 Satz 4 genannten Be-hörden nicht sachgerecht. Die Anwendbarkeit dieser Vorschrift war daher insoweit aus-zuschließen.*
	(3) [1]Auf die in § 6 Abs. 2 Satz 4 genannten Behörden findet Absatz 2 Satz 2 keine Anwendung. [2]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.	***Die Änderung*** [keine generelle Pflicht zur Herstellung des Benehmens mit dem Behördenleiter] ***trägt dem Vorschlag des Bundesrates (BR-Drs. 461/00 – Beschluss, S. 5, Nr. 5) weitgehend Rechnung.*** ***Bei den in § 6 Abs. 2 Satz 4 genannten Behörden muss der Vorbehalt des Benehmens mit dem verantwortlichen Behördenleiter jedoch beibehalten werden, da die Aufgabenerfüllung dieser Behörden die enge Begrenzung des Kreises der mit einer Angelegenheit befassten und über sie unterrichteten Personen erforderlich machen kann. Absatz 3 fasst den entsprechenden Vorbehalt mit der bereits in Absatz 2 Satz 4 des Regierungsentwurfs enthaltenen Ausnahme für diese Behörden zusammen.***
§ 5 a.F. Datengeheimnis	§ 5 n.F. Datengeheimnis	
Den bei der Datenverarbeitung beschäftig-	[1]Den bei der Datenverarbeitung beschäftig-	*In Satz 1 wurde das Wort „erheben“ aufgenommen, um den Anforderungen der Richt-linie*

ten Personen ist untersagt, personenbezogene Daten unbefugt zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Perso-nen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Auf-nahme ihrer Tätigkeit auf das Datenge-heimnis zu verpflichten. Das Datenge-heimnis besteht auch nach Beendigung ihrer Tätigkeit fort.	ten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). [2]Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. [3]Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.	*insoweit Rechnung zu tragen, als auch die Erhebung personenbezogener Daten im privaten Sektor dem Vorbehalt des Gesetzes zu unterstellen ist (vgl. hierzu auch die Begründung zu § 4 Abs. 1).*
§ 6 a. F.	§ 6 n.F.	
Unabdingbare Rechte des Betroffenen	Unabdingbare Rechte des Betroffenen	
(1) Die Rechte des Betroffenen auf Auskunft (§§ 19, 34) und auf Berichtigung, Löschung oder Sperrung (§§ 20, 35) können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.	(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) [1]Sind die Daten des Betroffenen in ei-ner Datei gespeichert, bei der mehrere Stellen speicherungsberechtigt sind, und ist der Betroffene nicht in der Lage, die speichernde Stelle festzustellen, so kann er sich an jede dieser Stellen wenden. [2]Diese ist verpflichtet, das Vorbringen des Betroffenen an die speichernde Stelle wei-terzuleiten. [3]Der Betroffene ist über die Weiterleitung und die speichernde Stelle zu unterrichten. [4]Die in § 19 Abs. 3 ge-nannten Stellen, die Behörden der Staats-anwaltschaft und der Polizei sowie öffent-liche Stellen der Finanzverwaltung, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwen-dungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, kön-nen statt des Betroffenen den Bundesbe-auftragten für den Datenschutz unterrichten. [5]In diesem Fall richtet sich das weite-re Verfahren nach § 19 Abs. 6.	(2) [1]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 Da-ten gespeichert hat, so kann er sich an jede dieser Stellen wenden. [2]Diese ist ver-pflichtet, das Vorbringen des Betroffenen an die Stelle, die die Daten gespeichert hat, weiterzuleiten. [3]Der Betroffene ist über die Weiterleitung und jene Stelle zu unterrichten. [4]Die in § 19 Abs. 3 genann-ten Stellen, die Behörden der Staatsan-waltschaft und der Polizei sowie öffentli-che Stellen der Finanzverwaltung, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwen-dungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, kön-nen statt des Betroffenen den Bundesbe-auftragten für den Datenschutz unterrich-ten. [5]In diesem Fall richtet sich das weite-re Verfahren nach	*Die Änderungen in Absatz 2 sind Folgeänderungen im Zusammenhang mit den Änderungen des Dateibegriffs (vgl. hierzu die Begründung zu § 3 Abs. 2) sowie der Erset-zung des Begriffs der speichernden Stelle durch den der verantwortlichen Stelle (vgl. hierzu die Begründung zu § 3 Abs. 7).*

§ 19 Abs. 6.

§ 6a n.F.

Automatisierte Einzelentscheidung

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

§ 6 a setzt Artikel 15 der Richtlinie um. Mit dieser Vorschrift soll verhindert werden, dass Entscheidungen aufgrund von Persönlichkeitsprofilen ergehen, ohne dass der Be-troffene die Möglichkeit hat, die zugrundeliegenden Angaben und Bewertungsmaßstäbe zu erfah-ren. Der Anwendungsbereich der Vorschrift ist dadurch eingeengt, dass es sich um eine Entscheidung handeln muss, die rechtliche Folgen nach sich zieht oder zumin-dest eine erheblich beeinträchtigende Wirkung hat. Vor allem aber muss die Entschei-dung aus-schließlich aufgrund einer automatisierten Verarbeitung erfolgen, d.h. eine er-neute Über-prüfung durch einen Menschen darf nicht vorgesehen sein. Im öffentlichen Bereich sind das in der Regel Verwaltungsakte. Nur in diesen Fällen greift das Verbot des Absatzes 1. Nach Artikel 15 Abs. 2 Buchstabe b der Richtlinie kann von dem Ver-bot durch einzel-staatliches Gesetz, das geeignete Garantien vorsieht, abgesehen wer-den.

Entscheidungen im Sinne des Absatzes 1 sind solche, die auf Daten gestützt werden, die zum Zweck der Bewertung einzelner Aspekte einer Person, wie beispielsweise ihrer beruflichen Leistungsfähigkeit, ihrer Kreditwürdigkeit, ihrer Zuverlässigkeit oder ihres Verhaltens, erhoben wurden. Hierunter sind insbesondere sog. Scoring-Verfahren, wie sie im Kreditgewerbe üblich sind, zu verstehen. Diese Verfahren, auch Punktwertver-fahren genannt, stellen eine Auswertungsmethode dar, eine Mehrzahl von Menschen oder Merk-malen in eine Reihenfolge nach einem oder mehreren Kriterien zu bringen, d.h. sie zu positionieren. Allerdings fallen Scoring-Verfahren nur dann unter die Rege-lung, wenn sowohl das Scoring-Verfahren als auch die anschließende Entscheidung in einer Hand liegen. **[siehe hierzu aber die Klarstellung in der Begründung zu § 34, unten S. 95]** *Keine Entscheidungen im Sinne des Absatzes 1 sind Vorgänge wie etwa Abhebungen am Geldausgabeautomaten, automatisierte Genehmigungen von Kreditkartenverfügungen oder automatisiert gesteuerte Guthabenabgleiche zur Ausführung von Überweisungs-, Scheck- oder Lastschriftaufträgen. Anlässlich der Geldtransaktion selbst wird lediglich ausgeführt, was in dem zugrundeliegenden Rechtsverhältnis zwischen Kreditinstitut und Kunde bereits vereinbart wurde. Auch bloße Vorentscheidungen, wie etwa die automati-sierte Vorauswahl im Vorfeld einer Personalbesetzung (automatisierter Abgleich des Personalbestandes anhand bestimmter Suchkriterien, wie etwa Alter, Ausbildung, Zu-satzqualifikation u. ä.), sind nicht erfasst.*

Identifikationsverfahren, etwa mittels Finger- oder Handabdrücken, der Iris oder der Stimme, werden von der Regelung ebenfalls nicht erfasst.

(2) Dies gilt nicht, wenn

1. die Entscheidung im Rahmen des Ab-

Absatz 2 setzt Artikel 15 Abs. 2 Buchstabe a der Richtlinie um und beinhaltet Ausnah-men von Absatz 1.

schlusses oder der Erfüllung eines Vertragsverhältnisses oder eines sonstigen Rechtsverhältnisses ergeht und dem Begehren des Betroffenen stattgegeben wurde oder	*Der Begriff des sonstigen Rechtsverhältnisses meint eine der ersten Alternative vergleichbare Fallgestaltung im öffentlichen Bereich.*
2. die Wahrung der berechtigten Interessen des Betroffenen durch geeignete Maßnahmen gewährleistet und dem Betroffenen von der verantwortlichen Stelle die Tatsache des Vorliegens einer Entscheidung im Sinne des Absatzes 1 mitgeteilt wird. Als geeignete Maßnahme gilt insbesondere die Möglichkeit des Betroffenen, seinen Standpunkt geltend zu machen. Die verantwortliche Stelle ist verpflichtet, ihre Ent-scheidung erneut zu prüfen.	*Als geeignete Maßnahme im Sinne des Absatzes 2 Nr. 2 gilt insbesondere die Möglichkeit des Betroffenen, seinen Standpunkt geltend zu machen. Daneben kommen auch andere Maßnahmen in Betracht. Maßstab ist insoweit die Effizienz der jeweiligen Maßnahme hinsichtlich der Wahrung des berechtigten Interesses der betroffenen Personen.* *Um dem Zweck der Regelung des Absatzes 2 Nr. 2 gerecht zu werden, muss der Betroffene über die Tatsache des Vorliegens einer Entscheidung im Sinne des Absatzes 1 informiert werden. Die erneute Überprüfung darf nicht ausschließlich automatisiert erfolgen.*
(3) Das Recht des Betroffenen auf Aus-kunft nach den §§ 19 und 34 erstreckt sich auch auf den logischen Aufbau der automatisierten Verarbeitung der ihn betreffen-den Daten.	*Absatz 3 setzt Artikel 12 Buchstabe a, 3. Spiegelstrich der Richtlinie um. Das Auskunftsrecht über den logischen Aufbau der automatisierten Verarbeitung soll Transparenz für den Betroffenen schaffen. Es zielt in erster Linie auf die Veranschaulichung dessen ab, was mit den Daten des Betroffenen geschieht. Nicht erfasst sind dagegen unter dem Gesichtspunkt des Schutzes des Geschäftsgeheimnisses beispielsweise Auskünfte über die verwendete Software. Dies wird in Erwägungsgrund 41 der Richt-linie deutlich. Der Anwendungsbereich dieses gegenüber dem bisherigen Recht erwei-terten Auskunftsrechts beschränkt sich auf die Fälle des § 6 a. Diese Einschränkung wird durch die zugrundeliegende Vorschrift der Richtlinie ermöglicht.*
§ 6b n.F. Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen	
(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie	*Die in weiten Bereichen durch öffentliche und nicht-öffentliche Stellen bereits durchgeführte Videoüberwachung öffentlich zugänglicher Räume erhält durch die Vorschrift eine gesetzliche Grundlage, die der Wahrung des informationellen Selbstbestimmungs-rechts durch einen angemessenen Interessensausgleich Rechnung trägt. Da bereits die Beobachtung selbst erfasst wird, kommt es nicht auf das Erfordernis einer anschließen-den Speicherung des Bildmaterials an, um datenschutzrechtlich relevant zu sein.*
1. zur Aufgabenerfüllung öffentlicher Stellen,	
2. zur Wahrnehmung des Hausrechts oder	*Die Vorschrift erfasst nur öffentlich zugängliche Räume wie etwa Bahnsteige, Ausstellungsräume eines Museums, Verkaufsräume oder Schalterhallen. Für nicht öffentlich*
3. zur Wahrnehmung berechtigter Interes-	

sen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.	*zugängliche Räume sind besondere Regelungen, beispielsweise im Rahmen eines Arbeitnehmerdatenschutzgesetzes, erforderlich.*
	Soweit in bereichsspezifischen Normen, etwa für die Polizei, den Bundesgrenzschutz und die Nachrichtendienste des Bundes, Rechtsgrundlagen zur Videoüberwachung und -aufzeichnung enthalten sind, bleiben diese unberührt.
(2) Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeigne-te Maßnahmen erkennbar zu machen.	*Absatz 2 dient der Transparenz des Vorgangs der Videoüberwachung. Geeignete Maßnahmen im Sinne dieser Vorschrift sind beispielsweise deutlich sichtbare Hinweisschilder. Zusätzlich zum Umstand der Beobachtung muss für den Betroffenen die verantwortliche Stelle erkennbar sein, damit dieser seine Rechte geltend machen kann.*
(3) [1]Die Verarbeitung oder Nutzung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. [2]Für einen anderen Zweck dürfen sie nur verarbeitet oder genutzt werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.	*Absatz 3 regelt die Speicherung der durch Beobachtung nach Absatz 1 erhobenen Daten. Die Speicherung ist nur zulässig, soweit sie für den verfolgten Zweck erforderlich ist.*
	Die Löschungsregelung des Absatzes 4 trägt auch einem vorrangigen Löschungsinteresse des Betroffenen Rechnung.
	§ 6b führt im BDSG erstmals eine verbindliche Reglementierung der Videoüberwachung ein. Sie findet für öffentliche Stellen des Bundes und für den nicht öffentlichen Bereich Anwendung.
	Neben § 6b gelten die sonstigen Vorschriften des Gesetzes, so etwa das in § 3a verankerte Gebot zur Datenvermeidung und Datensparsamkeit. Die besondere Eingriffsqualität, die von der Beobachtung öffentlich zugänglicher Räume ausgehen kann, macht erforderlich, zugunsten der von einer solchen Maßnahme betroffenen Personen den Kreis der eine Videoüberwachung rechtfertigenden Sachverhalte zu beschränken, eine enge Zweckbindung für die im Wege der Videoüberwachung gewonnenen personenbezogenen Daten vorzusehen und die Transparenz für die Betroffenen zu erhöhen.
(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über eine Verarbeitung oder Nutzung entsprechend §§ 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.	***Die besonderen Zulässigkeitsvoraussetzungen, die nach den Absätzen 1, 3 und 5 in den verschiedenen Verarbeitungsphasen jeweils gesondert zu prüfen sind, verfolgen – unter Berücksichtigung der im nicht öffentlichen Bereich zu beachtenden Grundrechtspositionen auch der Betreiber von Videotechnik, etwa aus Art. 12 und 14 GG – das Ziel, insgesamt eine restriktivere Verwendungspraxis herbeizuführen, ohne zugleich rechtlich schützenswerte Beobachtungszwecke auszuschließen.***
	Zu Absatz 1:
	In Nummer 1 wird durch den gegenüber dem Regierungsentwurf ergänzten Wortlaut („zur Aufgabenerfüllung öffentlicher Stellen“) klargestellt, dass diese Vorschrift – ebenso wie z. B. § 4 Abs. 2 Nr. 2 Buchstabe a, § 14 Abs. 1 Satz 1 und § 15 Abs. 1 Nr. 1 BDSG – nur für öffentliche Stellen im Rahmen ihrer gesetzlichen Aufgabenstellung gilt. Soweit bereichsspezifische Gesetze des Bundes Regelungen zur Vi-

deoüberwachung enthalten (z. B. § 21 Abs. 3, §§ 27 und 28 Abs. 2 BGSG, § 16 Abs. 1, § 23 Abs. 2 und § 26 BKAG sowie § 8 Abs. 2 Satz 1 i.V.m. § 9 BVerfSchG), sind diese abschließend, so dass insoweit durch § 6b keine zusätzlichen Eingriffsbefugnisse normiert werden.

Der Zweck „Wahrnehmung des Hausrechts“ (Nummer 2) erfasst den Einsatz von Videotechnik sowohl durch öffentliche als auch durch nicht öffentliche Stellen.

Nummer 3 („zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke“), der allein den nicht öffentlichen Bereich betrifft, führt gegenüber dem Regierungsentwurf („Erfüllung eigener Geschäftszwecke“) zu einer Einschränkung der Zulässigkeit der Videoüberwachung. Der Begriff „Wahrnehmung berechtigter Interessen“ ist § 28 Abs. 1 Satz 1 Nr. 2 entlehnt, der als Ausnahmetatbestand eng auszulegen ist. Was ein berechtigtes Interesse der verantwortlichen Stelle sein kann, bestimmt sich nicht allein nach deren subjektiven Interesse, z.B. durch Definition eines Geschäftszwecks, sondern muss objektiv begründbar sein. Von einer Wahrnehmung berechtigter Interessen kann regelmäßig nicht ausgegangen werden, wenn die Beobachtung der Hauptzweck oder ein wesentlicher Nebenzweck der Geschäftstätigkeit ist. So wäre etwa eine Videoüberwachung mit dem Ziel der Vermarktung hierdurch gewonnener Bilder unzulässig.

Entsprechend § 28 Abs. 1 Satz 2 schreibt Nummer 3 in der gegenüber dem Regierungsentwurf ergänzten Fassung vor, die Zwecke der Videoüberwachung vor Beginn dieser Maßnahme konkret festzulegen. Hierdurch wird die Nachprüfung der Erforderlichkeit der jeweiligen Beobachtungsmaßnahme – etwa im Hinblick auf die eingesetzte Technik – erleichtert.

Die Verfolgung eines zulässigen Zwecks im Sinne des Absatzes 1 ist allein jedoch nicht ausreichend für die Zulässigkeit einer Videoüberwachung. Vielmehr können auch in diesem Fall entgegenstehende Interessen Betroffener zu einem Ausschluss dieser Maßnahme führen. So kann etwa der Zweck der Diebstahlsprävention in keinem Fall die Überwachung von Toiletten oder Umkleidekabinen rechtfertigen.

Absatz 1 greift insoweit über den Anwendungsbereich des BDSG, wie er in § 1 Abs. 2 Nr. 3 definiert ist, hinaus, als er nicht voraussetzt, dass die durch eine Beobachtungsmaßnahme gewonnenen Daten unter Einsatz von oder für Datenverarbeitungsanlagen erhoben werden. Insbesondere beim Einsatz digitaler Kameratechnik wird dies jedoch regelmäßig der Fall sein.

Zu Absatz 2:

Die Pflicht zur Erkennbarmachung der Beobachtung und zur Nennung der verantwortlichen Stelle ergänzt die nach dem Gesetz bestehenden allgemeinen Verfahrenssicherungen. So löst die als automatisierte Verarbeitung erfolgende Video-

überwachung die Meldepflicht nach § 4d Abs. 1 aus.

Videoüberwachungen, die besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, unterliegen darüber hinaus der Vorabkontrolle nach § 4d Abs. 5. Solche besonderen Risiken liegen regelmäßig vor, wenn Überwachungskameras nicht punktuell, sondern durch die verantwortliche Stelle in größerer Zahl und zentral kontrolliert eingesetzt werden. Ebenso kann die verwendete Technik (etwa bei schwenkbaren Kameras mit hoher Auflösung der gewonnenen Bilder) zu einem solchen besonderen Risiko führen.

Zu Absatz 3:

Absatz 3 führt besondere Zulässigkeitsvoraussetzungen für die Verarbeitung und Nutzung der im Wege der Videoüberwachung gewonnenen personenbezogenen Daten ein. Aus der Zulässigkeit der Beobachtung nach Absatz 1 kann nicht bereits auf die Zulässigkeit der Verarbeitung oder Nutzung gewonnener personenbezogener Daten geschlossen werden. Vielmehr muss nach Absatz 3 in einem eigenen Prüfschritt festgestellt werden, ob gerade auch die in Aussicht genommene Verarbeitung oder Nutzung zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen des Betroffenen überwiegen (Satz 1), oder ob die Verwendung für Gefahrenabwehr- oder Strafverfolgungszwecke erforderlich ist (Satz 2).

Insbesondere bei Anwendung digitaler Videoüberwachungssysteme kommt der Abwägungsklausel herausragende Bedeutung zu. Für jeden Schritt der Verarbeitung und Nutzung von Videomaterial ist eine gesonderte Bewertung der Zulässigkeit geboten. Schutzwürdige Interessen der Betroffenen sind in besonderer Weise berührt, wenn automatisierte Verfahren beispielsweise zum Vergrößern und Herausfiltern einzelner Personen, zur biometrischen Erkennung, zum Bildabgleich oder zur Profilerstellung eingesetzt werden oder in dem zur Videoüber-wachung eingesetzten System verfügbar und einsatzbereit sind. Denn derartige Maßnahmen greifen in besonders gravierender Weise in das informationelle Selbstbestimmungsrecht der Betroffenen ein. Regelmäßig überwiegt insofern das Interesse der Betroffenen, nicht zum Objekt automatisierter Verarbeitung sie betreffender Videoaufnahmen zu werden. Nur ausnahmsweise kann der Einsatz automatisierter Systeme zur Erkennung von Personen in Betracht kommen, etwa wenn der zulässige Zweck nicht auf andere Weise wirksam erreicht werden kann. Der Vorabkontrolle (vgl. oben zu Absatz 2) kommt hier in besonderer Weise eine verfahrenssichernde Funktion zu.

Je leistungsfähiger die Möglichkeiten automatisierter Auswertung von Videoaufnahmen von Personen im Zuge technologischer Fortentwicklung werden, desto gewichtiger ist das informationelle Selbstbestimmungsrecht im Rahmen der Abwä-

gung zu Gunsten der Betroffenen zu berücksichtigen.

In der Fassung des Änderungsantrags führt Absatz 3 zu einer Erstreckung der Zweckbindung der im Wege der Videoüberwachung gewonnenen personenbezogenen Daten über die Phase der Speicherung hinaus auch auf alle übrigen Phasen der Verarbeitung und die Nutzung. Grundsätzlich dürfen aus der Videoüberwachung gewonnene personenbezogene Daten nur für den originären Beobachtungszweck verarbeitet und genutzt werden. Eine Ausnahme sieht Satz 2 (anknüpfend an § 28 Abs. 3 Nr. 2) ausschließlich zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten vor (Beispiel: ein Passant wird in einer videoüberwachten Ladenpassage überfallen). Ein Rückgriff auf die weiteren in § 28 Abs. 3 (bzw. § 14 Abs. 2 bis 6) enthaltenen Tatbestände zulässiger Zweckänderung bleibt ausgeschlossen. Unzulässig ist danach etwa die zweckändernde Herausgabe oder Nutzung von Videomaterial zur Wahrnehmung berechtigter Interessen eines Dritten (vgl. § 28 Abs. 3 Nr. 1) oder für Werbungszwecke (vgl. § 28 Abs. 3 Nr. 3).

Zu Absatz 4:

Der neu eingefügte Absatz 4 trägt zur Transparenz der Verarbeitung und Nutzung von durch Videoüberwachung gewonnenen personenbezogenen Daten bei. Die Zuordnung erhobenen Daten zu einer bestimmten Person wird regelmäßig die Benachrichtigungspflicht nach den §§ 19a und 33 auslösen. Eine ausdrückliche Verweisung ist im Rahmen des § 6b jedoch sinnvoll, weil die Vorschrift auch solche Fallgestaltungen erfasst, in denen Daten durch analoge Videotechnik – also nicht im Wege einer automatisierten Verarbeitung – gewonnen werden.

Zu Absatz 5:

Absatz 5 entspricht Absatz 4 des Regierungsentwurfs. Videomaterial, das für den Beobachtungszweck nicht mehr benötigt wird, ist unverzüglich zu löschen. Aber auch Videomaterial, das für den Beobachtungszweck noch benötigt wird, etwa weil aufklärungsbedürftige Vorkommnisse erfasst wurden, darf nur gespeichert bleiben, wenn schutzwürdige Interessen des Betroffenen nicht entgegenstehen und solange es zur Erreichung des Beobachtungszwecks erforderlich ist.

Aus dieser zweifachen Ausrichtung des Löschungsgebots folgt die Verpflichtung der verantwortlichen Stelle, die Prüfung angefallenen Videomaterials zur Bedarfsklärung unverzüglich, d.h. in der Regel innerhalb von ein bis zwei Arbeitstagen, vorzunehmen. Am wirksamsten wird dem Löschungsgebot durch eine automatisierte periodische Löschung, etwa durch Selbstüberschreiben zurückliegender Aufnahmen, entsprochen. Dem Grundsatz der Datenvermeidung und Datensparsamkeit (§ 3a) kommt in diesem Zusammenhang maßgebliche Bedeutung zu.

Nach der in kurzer Frist zu erfolgenden Bedarfsklärung darf daher nach Absatz 1

	gewonnenes Videomaterial nur noch insoweit vorhanden sein, als es sich um relevante Aufnahmen handelt, die für den Beobachtungszweck weiter benötigt werden und deren Speicherung schutzwürdige Interessen des Betroffenen nicht entgegen stehen. Ein sich anschließendes Verfahren zur Aufklärung oder Verfolgung von Vorkommnissen ist zügig zu betreiben, um die Löschung der verbliebenen Daten nicht unangemessen zu verzögern.
§ 6c Mobile personenbezogene Speicher- und Verarbeitungsmedien	
(1) Die Stelle, die ein mobiles personenbezogenes Speicher- und Verarbeitungsmedium ausgibt oder ein Verfahren zur automatisierten Verarbeitung personenbezoge-ner Daten, das ganz oder teilweise auf ei-nem solchen Medium abläuft, auf das Me-dium 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.	***Mobile personenbezogene Speicher- und Verarbeitungsmedien (vgl. § 3 Abs. 10) zeichnen sich dadurch aus, dass personenbezogene Daten auf ihnen nicht nur gespeichert, sondern auch verarbeitet werden können, ohne dass diese Verarbeitungsvorgänge für den Betroffenen unmittelbar nachvollziehbar sind. § 6c schafft die im Hinblick auf das informationelle Selbstbestimmungsrecht des Betroffenen gebotene Transparenz, indem sowohl der ausgebenden Stelle als auch allen Stellen, die auf das Medium Verarbeitungsverfahren aufbringen, Unterrichtungspflichten auferlegt werden. § 6c knüpft bereits an den Vorgang der Ausgabe eines Mediums oder die Aufbringung eines Verarbeitungsverfahrens an, ohne dass es darauf ankommt, ob sogleich personenbezogene Daten gespeichert wer-den. Der Betroffene soll von Anfang an die Funktionalität des Mediums und der Verfahren kennen, um bereits vor dem ersten Speichern personenbezogener Da-ten die Bedeutung und Tragweite des Verfahrens erkennen zu können. Dadurch erst wird es ihm möglich, informiert zu entscheiden, ob er seine personenbezogenen Daten einem Verfahren unter Einsatz des Mediums anvertrauen will.*** ***Normadressat von § 6c ist die Stelle, die ein Medium nach § 3 Abs. 10 ausgibt oder ein Verfahren nach § 6c Abs. 1 aufbringt oder ändert. Einbezogen werden auch Stellen, die solche Verfahren zur Aufbringung durch den Karteninhaber – etwa im Wege des Herunterladens aus dem Internet – bereithalten.***
(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.	***Aus § 3a und § 9 i.V.m. der zugehörigen Anlage leiten sich Rahmenbedingungen für die technische Gestaltung des Mediums und die Konzeption der aufzubringenden Verfahren ab. So müssen die in § 3 Abs. 2 genannten Geräte und Einrichtungen so aufgestellt sein, dass die Auskünfte, die der Betroffene durch sie erlangt, nicht auch von Dritten, etwa umstehenden Personen, wahrgenommen werden können. Das gleiche gilt, wenn beim Gebrauch der Karte im Zusammenhang mit der nach § 3 Abs. 3 vorgeschriebenen Signalisierung eines Verarbeitungsvorgangs personenbezogene Daten zur Transparenz und Kontrolle für den Betroffenen angezeigt werden.***
(3) Kommunikationsvorgänge, die auf dem	

Medium eine Datenverarbeitung auslösen, müssen für den Betroffenen eindeutig erkennbar sein.

Zu Absatz 1:

Die Angaben nach Absatz 1 Nr. 1 sind erforderlich, damit der Betroffene seine Rechte gegenüber der verpflichteten Stelle geltend machen kann.

Zentrale Bedeutung kommt der Unterrichtung des Betroffenen über die Funktionsweise des Mediums (Absatz 1 Nr. 2) zu. Der gebotene Umfang der Unterrichtung wird von ihrem Zweck bestimmt, erkennbar zu machen, wie personenbezogene Daten verarbeitet werden können. Die Unterrichtung muss „in allgemein verständlicher Form“ erfolgen. Detaillierte technische Beschreibungen werden dem nicht gerecht; andererseits können sie nach dieser Vorschrift auch nicht beansprucht werden.

Bei Ausgabe eines Mediums, auf das noch keine Verfahren aufgebracht sind, ist darüber zu unterrichten, dass es sich um ein Medium mit Prozessorchip handelt, auf das Verfahren zur automatisierten Verarbeitung personenbezogener Daten aufgebracht werden können. Hierbei ist beispielsweise über die Verwendung eines karten- und maschinenunabhängigen Programmiercodes (etwa: Java-Fä-higkeit) und allgemein über das Verwendungspotenzial des Mediums bei Aufbringung entsprechender Verfahren zu unterrichten. Ferner muss der Betroffene Kenntnis erlangen, wie Verfahren auf das Medium aufgebracht werden können (beispielsweise: berührungslos an einem Lese- und Schreibgerät). Der Betroffene soll Möglichkeiten und Risiken des Mediums im Blick auf sein informationelles Selbstbestimmungsrecht erkennen können.

Das Aufbringen eines Verfahrens zur automatisierten Verarbeitung personenbezogener Daten, das ganz oder teilweise auf einem mobilen personenbezogenen Speicher- und Verarbeitungsmedium abläuft, ist der zweite Tatbestand, der die Unterrichtungspflicht auslöst. Er wird erfüllt, wenn auf dem Medium die konkreten Vorkehrungen dafür getroffen werden, dass die automatisierte Verarbeitung personenbezogener Daten im Rahmen eines Verfahrens erfolgen kann. Typischerweise erfolgt das durch Speichern eines Programmcodes auf dem Medium und die Reservierung eines Speicherbereichs. Nach Absatz 1 Nr. 2 ist über die nach Aufbringung des Verfahrens erweiterte Funktionsweise des Mediums zu unterrichten, konkret also über die Funktion des aufgebrachten Verfahrens. Wie sich aus der Formulierung „Verfahren, ... das ganz oder teilweise auf dem ... Medium abläuft“ ergibt, ist Anknüpfungspunkt das Verfahren insgesamt, einschließlich außerhalb des Mediums ablaufender Teile und einschließlich einzelner bei bestimmten Sachverhalten etwa manuell vorzunehmender Entscheidungen. Andererseits genügt eine Unterrichtung über die im Blick auf das informationelle Selbstbestimmungsrecht prak-

tisch relevanten Verarbeitungsoptionen.

Die Unterrichtungspflicht nach Absatz 1 Nr. 3 bezieht sich nicht unmittelbar auf die personenbezogenen Daten, sondern darauf, wie der Betroffene seine Rechte nach den §§ 19, 20, 34 und 35 im Hinblick auf Besonderheiten des Mediums ausüben kann. Die Unterrichtung muss sich insbesondere auf die Standorte und Funktion der Geräte oder Einrichtungen nach Absatz 2 beziehen. Die ausschließliche Erwähnung der §§ 19, 20, 34 und 35 lässt die Benachrichtigungspflichten nach §§ 19a und 33 (denen keine Rechte des Betroffenen gegenüberstehen, die von ihm im Sinne von Absatz 1 Nr. 3 „ausgeübt“ werden könnten) und alle übrigen Rechte des Betroffenen und Pflichten der verantwortlichen Stelle nach diesem Gesetz unberührt.

Zu unterrichten ist auch über die bei Verlust oder Zerstörung des Mediums zu treffenden Maßnahmen, Absatz 1 Nr. 4.

Der letzte Halbsatz von Absatz 1 reduziert den Unterrichtungsaufwand bei Verfahrensänderungen auf den tatsächlichen Umfang der Änderungen. Es liegt in der Eigenverantwortung des Betroffenen, ihm ausgehändigte Handzettel und Broschüren aufzubewahren bzw. sich Notizen über erfolgte Unterrichtungen zu machen.

Zu Absatz 2:

Bereits in den allgemeinen Vorschriften über das Auskunftsrecht des Betroffenen ist die Unentgeltlichkeit der Auskunft vorgeschrieben (§ 19 Abs. 7, § 34 Abs. 5 Satz 1). Absatz 2 konkretisiert und ergänzt diese Vorschriften für Medien nach § 3 Abs. 10. Die Auskunft muss danach auch dann unentgeltlich bleiben, wenn zur Wahrnehmung des Auskunftsrechts hinsichtlich der auf dem Medium gespeicherten personenbezogenen Daten Geräte oder Einrichtungen erforder-lich sind; solche erforderlichen Geräte oder Einrichtungen müssen in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung stehen. Der unbestimmte Rechtsbegriff „in angemessenem Umfang“ ermöglicht die insbesondere im Hinblick auf die Sensibilität der im Einzelfall betroffenen personenbezogenen Daten, den wirtschaftlichen Aufwand, die Verbreitung eines Verfahrens und den technischen Fortschritt gebotene flexible Rechtsanwendung. Nicht jedes Lese- und/oder Schreibgerät, mit dem das Medium kommuniziert, muss über die in Ab-satz 2 angesprochene Auskunftsfunktion verfügen. Absatz 2 beschränkt die Unentgeltlichkeit auf den „Gebrauch“ der erforderlichen Geräte oder Einrichtungen. Ein Anspruch auf Übereignung oder auf Einräumung des – die Nutzung durch andere Personen ausschließenden – eigenen Besitzes wird durch Absatz 2 nicht begründet.

Zu Absatz 3:

Während Absatz 1 zur einmaligen Unterrichtung bei der Ausgabe eines Mediums und bei der erstmaligen Aufbringung oder späteren Änderung eines Verfahrens auf

		das Medium verpflichtet, bezieht sich Absatz 3 auf einzelne Anwendungsfälle, in denen Kommunikationsvorgänge auf dem Medium eine Datenverarbeitung auslösen. Die Regelung ergänzt die Unterrichtungspflichten nach Absatz 1 und soll sicherstellen, dass Verarbeitungen nicht unbemerkt, z.B. beim Vorbeigehen an einem Terminal, ausgelöst werden.
§ 7 a.F.	§ 7 n.F.	
Schadensersatz durch öffentliche Stellen	Schadensersatz	
(1) Fügt eine öffentliche Stelle dem Betroffenen durch eine nach den Vorschriften dieses Gesetzes oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige automatisierte Verarbeitung seiner personenbezogenen Daten einen Schaden zu, ist sie dem Betroffenen unabhängig von einem Verschulden zum Ersatz des daraus entstehenden Schadens verpflichtet.	[1]Fügt eine verantwortliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist sie oder ihr Träger dem Betroffenen zum Schadensersatz verpflichtet. [2]Die Ersatzpflicht entfällt, soweit die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.	*Im Gegensatz zur Regelung der §§ 7 und 8 a.F. wird in Umsetzung von Artikel 23 der Richtlinie in Satz 1 erstmals eine eigenständige Anspruchsgrundlage im Bundesdatenschutzgesetz für eine Verschuldenshaftung geschaffen, die sowohl im öffentlichen als auch im nicht-öffentlichen Bereich gilt. Sie umfasst sowohl Schadensersatzansprüche aus automatisierter als auch aus nicht-automatisierter Datenverarbeitung. Satz 2 setzt Artikel 23 Abs. 2 der Richtlinie um, der den für die Verarbeitung Verantwortlichen von der Haftung befreit, wenn er nachweist, dass der Umstand, durch den der Schaden eingetreten ist, ihm nicht zur Last gelegt werden kann. Er erfasst erstmals auch den öffentlichen Bereich und dort auch Ansprüche aus fehlerhafter nicht-automatisierter Datenverarbeitung und findet damit auch bei der Datenverarbeitung in Akten Anwendung.* *Da Artikel 2 Buchstabe b der Richtlinie auch die Erhebung und Nutzung in den Verarbeitungsbegriff einbezieht, war die Vorschrift entsprechend zu ergänzen.*
(2) Bei einer schweren Verletzung des Persönlichkeitsrechts ist dem Betroffenen der Schaden, der nicht Vermögensschaden ist, angemessen in Geld zu ersetzen.		*Absatz 2 entspricht Absatz 5 a.F., Absatz 3 entspricht Absatz 7 a.F. und Absatz 4 entspricht Absatz 8 a.F.* ***Die Änderung zu § 7 folgt dem Vorschlag des Bundesrates (BR-Drs. 461/00 – Beschluss, S. 6, Nr. 6. a), die in Absatz 1 Satz 2 geregelte Beweislastverteilung dadurch zu verdeutlichen, dass in Satz 1 das Wort „schuldhaft“ gestrichen wird. Die Einfügung der Wörter „sie oder“, ebenfalls in Satz 1, soll dem Umstand Rechnung tragen, dass bei juristischen Personen des Privatrechts eine Haftung des Trägers nicht in Betracht kommt.*** ***Der Bundesrat hat zu § 7 außerdem geltend gemacht, dass die Absätze 2 bis 4 entbehrlich sind, da § 7 einen deliktischen Anspruch zum Gegenstand hat.*** ***Die Bundesregierung hat in ihrer Gegenäußerung zur Stellungnahme des Bundesrates (Drs. 14/4458, vgl. dort zu Nr. 6 Buchstabe b) darauf hingewiesen, dass die Regelungstatbestände des § 7 Abs. 2 bis 4 im Rahmen der von § 8 geregelten Gefährdungshaftung ebenfalls nur deklaratorische Bedeutung haben. Dementsprechend kann auch die in § 8 Abs. 6*** [des RegE] ***enthaltene Verweisungsnorm entfallen.***
(3) [1]Die Ansprüche nach den Absätzen 1 und 2 sind insgesamt bis zu einem Betrag		

in Höhe von zweihundertfünfzigtausend Deutsche Mark begrenzt. [2]Ist aufgrund desselben Ereignisses an mehrere Personen Schadensersatz zu leisten, der insgesamt den Höchstbetrag von zweihundertfünfzigtausend Deutsche Mark übersteigt, so verringern sich die einzelnen Schadensersatzleistungen in dem Verhältnis, in dem ihr Gesamtbetrag zu dem Höchstbetrag steht.		
(4) Sind bei einer Datei mehrere Stellen speicherungsberechtigt und ist der Geschädigte nicht in der Lage, die speichernde Stelle festzustellen, so haftet jede dieser Stellen.		
(5) Mehrere Ersatzpflichtige haften als Gesamtschuldner.		
(6) Auf das Mitverschulden des Betroffe-nen und die Verjährung sind die §§ 254 und 852 des Bürgerlichen Gesetzbuches entsprechend anzuwenden.		
(7) Vorschriften, nach denen ein Ersatzpflichtiger in weiterem Umfang als nach dieser Vorschrift haftet oder nach denen ein anderer für den Schaden verantwort-lich ist, bleiben unberührt.		
(8) Der Rechtsweg vor den ordentlichen Gerichten steht offen.		
§ 8 a.F.	§ 8 n.F.	
Schadensersatz durch nicht-öffentliche Stellen	Schadensersatz bei automatisierter Datenverarbeitung durch öffentliche Stellen	
Macht ein Betroffener gegenüber einer nicht-öffentlichen Stelle einen Anspruch auf Schadensersatz wegen einer nach die-sem Gesetz oder anderen Vorschriften über den Datenschutz unzulässigen oder unrichtigen	(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,	*§ 8 entspricht im Wesentlichen § 7 a.F.*

automatisierten Datenverarbei-tung geltend und ist streitig, ob der Scha-den die Folge eines von der speichernden Stelle zu vertretenden Umstandes ist, so trifft die Beweislast die speichernde Stelle.	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 Vermögensscha-den ist, angemessen in Geld zu ersetzen. (3) [1]Die Ansprüche nach den Absätzen 1 und 2 sind insgesamt auf einen Betrag von 250 000 Deutsche Mark begrenzt. [2]Ist aufgrund desselben Ereignisses an mehrere Personen Schadensersatz zu leisten, der insgesamt den Höchstbetrag von 250 000 Deutsche Mark 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) Auf das Mitverschulden des Betroffenen und die Verjährung sind die §§ 254 und 852 des Bürgerlichen Gesetzbuches entsprechend anzuwenden.	
§ 9 a.F. Technische und organisatorische Maßnahmen	§ 9 n.F. Technische und organisatorische Maßnahmen	
[1]Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezo-gene Daten verarbeiten, haben die techni-schen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Geset-zes, insbe-	[1]Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezo-gene Daten erheben, verarbeiten oder nut-zen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschrif-	*Da Artikel 2 Buchstabe b der Richtlinie auch die Erhebung und Nutzung in den Verarbeitungsbegriff einbezieht, war die Vorschrift entsprechend zu ergänzen.*

sondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. [2]Erforderlich sind Maß-nahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem ange-strebten Schutzzweck steht.	ten dieses Gesetzes, insbesonde-re die in der Anlage zu diesem Gesetz ge-nannten Anforderungen, zu gewährleisten. [2]Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.	
	§ 9a n.F. Datenschutzaudit	
	[1]Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und –programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und be-werten lassen sowie das Ergebnis der Prü-fung veröffentlichen. [2]Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt.	*Das Datenschutzaudit verfolgt das Ziel, datenschutzfreundliche Produkte auf dem Markt zu fördern, indem deren Datenschutzkonzept geprüft und bewertet wird. Eine entsprechende Regelung zum Datenschutzaudit enthält § 17 Mediendienste-Staatsver-trag.* *Satz 2 bestimmt für das nähere Verfahren des Audits eine Regelung durch Gesetz. Dies ist notwendig, da die Bestimmung der Anforderungen an die Prüfung und Bewer-tung sowie die Auswahl und Zulassung der Gutachter berufsbeschränkenden Charak-ter hat und damit dem verfassungsrechtlichen Vorbehalt des Gesetzes unterliegt.*
§ 10 a.F. Einrichtung automatisierter Abrufverfahren	§ 10 n.F. Einrichtung automatisierter Abrufverfahren	
(1) [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. [2]Die Vorschriften über die Zulässigkeit des einzelnen Abrufs bleiben unberührt.	(1) [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. [2]Die Vorschriften über die Zulässigkeit des einzelnen Abrufs bleiben unberührt.	*Beim Abruf handelt es sich um eine Form der Übermittlung. § 10 gilt daher nur für Online-Verfahren der verantwortlichen Stelle mit Dritten. Da der Begriff des Empfängers nun in § 3 Abs. 8 Satz 1 definiert ist, war Absatz 2 Nr. 2 durch den Begriff des Dritten zu präzisieren.* *Entsprechendes gilt für die Neuformulierung von Absatz 4.*
(2) [1]Die beteiligten Stellen haben zu gewährleisten, daß die Zulässigkeit des Ab-	(2) [1]Die beteiligten Stellen haben zu gewährleisten, dass die Zulässigkeit des Ab-	

rufverfahrens kontrolliert werden kann. [2]Hierzu haben sie schriftlich festzulegen:	rufverfahrens kontrolliert werden kann. [2]Hierzu haben sie schriftlich festzulegen:	
1. Anlaß und Zweck des Abrufverfahrens,	1. Anlass und Zweck des Abrufverfahrens,	
2. Datenempfänger,	2. Dritte, an die übermittelt wird,	
3. Art der zu übermittelnden Daten,	3. Art der zu übermittelnden Daten,	
4. nach § 9 erforderliche technische und organisatorische Maßnahmen.	4. nach § 9 erforderliche technische und organisatorische Maßnahmen.	
[3]Im öffentlichen Bereich können die erforderlichen Festlegungen auch durch die Fachaufsichtsbehörden getroffen werden.	[3]Im öffentlichen Bereich können die erforderlichen Festlegungen auch durch die Fachaufsichtsbehörden getroffen werden.	
(3) [1]Über die Einrichtung von Abrufverfah-ren ist in Fällen, in denen die in § 12 Abs. 1 genannten Stellen beteiligt sind, der Bundesbeauftragte für den Datenschutz unter Mitteilung der Festlegungen nach Absatz 2 zu unterrichten. [2]Die Einrichtung von Abrufverfahren, bei denen die in § 6 Abs. 2 und in § 19 Abs. 3 genannten Stel-len beteiligt sind, ist nur zulässig, wenn der für die speichernde und die abrufende Stelle jeweils zuständige Bundes- oder Landesminister oder deren Vertreter zuge-stimmt haben.	(3) [1]Über die Einrichtung von Abrufverfah-ren ist in Fällen, in denen die in § 12 Abs. 1 genannten Stellen beteiligt sind, der Bundesbeauftragte für den Datenschutz unter Mitteilung der Festlegungen nach Absatz 2 zu unterrichten. [2]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.	*Die Änderungen in Absatz 3 Satz 2 sowie die Streichung der Worte „oder deren Vertreter“ geht auf einen Beschluss des Bundeskabinetts vom 20. Januar 1993 (GMBl. S. 46) zurück, nach dem einheitlich für alle Bundesressorts die sächliche Bezeichnungsform einzuführen ist. Auch in den Ländern ist die sächliche Bezeichnungsform für die Landesressorts eingeführt worden.*
(4) [1]Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt der Empfänger. [2]Die speichernde Stelle prüft die Zulässigkeit der Abrufe nur, wenn dazu Anlaß besteht. [3]Die speichernde Stelle hat zu gewährleisten, daß die Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann. [4]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.	(4) [1]Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt der Dritte, an den übermittelt wird. [2]Die speichernde Stelle prüft die Zulässigkeit der Abrufe nur, wenn dazu Anlass besteht. [3]Die speichern-de Stelle hat zu gewährleisten, dass die Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann. [4]Wird ein Gesamtbestand personenbezogener Daten abgerufen oder übermittelt (Stapelverarbeitung), so be-zieht sich die Gewährleistung der Feststel-lung und Überprüfung nur auf die Zulässig-keit des Abrufes oder der Übermittlung des Gesamtbestandes.	

(5) Die Absätze 1 bis 4 gelten nicht für den Abruf aus Datenbeständen, die jedermann, sei es ohne oder nach besonderer Zulassung, zur Benutzung offenstehen.	(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.	***Der Bundesrat hat bei der von ihm angeregten Neufassung der Straf- und Bußgeldvorschriften die Ersetzung des Begriffs „offenkundig“ durch „allgemein zugänglich“ vorgeschlagen. Soweit dem gefolgt wird, empfiehlt sich insgesamt die Verwendung eines einheitlichen Sprachgebrauchs, da Bedeutungsunterschiede zwischen den Formulierungen „Datenbestände, die jedermann ... offen stehen“ (§ 10 Abs. 5 der geltenden Gesetzesfassung), "Daten aus allgemein zugänglichen Quellen" (§ 14 Abs. 2 Nr. 5 und § 28 Abs. 1 Satz 1 Nr. 3 i. d. F. des Regierungsentwurfs) und „Daten, die allgemein zugänglich sind" (vgl. Vorschlag des Bundesrates zu § 43 Abs. 1 und 2 Nr. 1) und „Daten, die ... offenkundig sind" (§ 43 Abs. 1 und 2 Nr. 1 i. d. F. des Regierungsentwurfs) nicht bestehen.***
§ 11 a.F.	§ 11 n.F.	
Verarbeitung oder Nutzung personenbezogener Daten im Auftrag	Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag	
(1) [1]Werden personenbezogene Daten im Auftrag durch andere Stellen verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. [2]Die in den §§ 6 bis 8 genannten Rechte sind ihm gegenüber geltend zu machen.	(1) [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. [2]Die in den §§ 6, 7 und 8 genannten Rechte sind ihm gegenüber geltend zu machen.	*Da Artikel 2 Buchstabe b der Richtlinie auch die Erhebung und Nutzung in den Verarbeitungsbegriff einbezieht, war die Vorschrift entsprechend zu ergänzen.* *Die Änderung in Absatz 1 Satz 2 ist eine Folgeänderung der neu eingefügten Vorschriften der §§ 6 a ff.*
(2) [1]Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. [2]Der Auftrag ist schriftlich zu erteilen, wobei die Datenverarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind. [3]Er kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden.	(2) [1]Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. [2]Der Auftrag ist schriftlich zu erteilen, wobei die Datenerhebung, -verarbei-tung oder -nutzung, die technischen und organisatorischen Maßnahmen und etwai-ge Unterauftragsverhältnisse festzulegen sind. [3]Er kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde er-teilt werden. [4]Der Auftraggeber hat sich von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.	*Absatz 2 Satz 4 setzt Artikel 17 Abs. 2 zweiter Halbsatz der Richtlinie um.* ***Die Änderung*** [Umstellung des Satzes 4] ***setzt einen Vorschlag des Bundesrates (Drs. 461/00 – Beschluss, S.7 zu Nr. 8) um. Der Bundesrat hat darauf hingewiesen, dass die Verpflichtung des Auftraggebers, sich von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen zu überzeugen, nicht zwingend „beim“ Auftragnehmer vor Ort erfüllt werden muss.*** ***Die vom Bundesrat zusätzlich für erforderlich gehaltene Klarstellung „in geeigneter Weise“ ist dagegen entbehrlich, da es keiner gesetzlichen Klarstellung be-darf, dass der Auftragnehmer seine gesetzlichen Verpflichtungen nur durch geeignete Maßnahmen erfüllen kann (vgl. Gegenäußerung der Bundesregierung, Drs. 14/4458, S. 2 zu Nr. 8).***
(3) [1]Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftrag-	(3) [1]Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftrag-	

gebers verarbeiten oder nutzen. [2]Ist er der Ansicht, daß eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüg-lich darauf hinzuweisen.	gebers erheben, verarbeiten oder nutzen. [2]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, Abs. 3 und 4 sowie 44 Abs. 1 Nr. 2, 5, 6 und 7 und Abs. 2 nur die Vorschriften über die Datenschutzkon-trolle oder die Aufsicht, und zwar für	(4) Für den Auftragnehmer gelten neben den §§ 5, 9, 43 Abs. 1, Abs. 3 und 4 sowie § 44 Abs. 1 Nr. 2, 5, 6 und 7 und Abs. 2 nur die Vorschriften über die Datenschutz-kontrolle 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 Datenschutz-gesetze der Länder,	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 Dienstleistungsunterneh-men geschäftsmäßig verarbeiten oder nutzen, die §§ 32, 36 bis 38.	2. die übrigen nicht öffentlichen Stellen, soweit sie personenbezogene Daten im Auftrag als Dienstleistungsunternehmen geschäftsmäßig erheben, verar-beiten oder nutzen, die §§ 4 f , 4 g und 38.	*Die geänderten Verweise in Absatz 4 Nr. 2 sind Folgeänderungen im Zusammenhang mit den Aufhebungen der §§ 32, 36 und 37, dem Entfallen der Meldepflicht für die Auftragsdatenverarbeitung im nicht-öffentlichen Bereich (§ 4 d Abs. 4) sowie mit der Schaffung der neuen Vorschriften der §§ 4 f und 4 g.*
	(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 da-bei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.	*Die Vorschrift erklärt die Regelungen über die Auftragsdatenverarbeitung der Absätze 1 bis 4 für entsprechend anwendbar auf die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch Stellen außerhalb der verantwortli-chen Stelle.*

Zweiter Abschnitt **Datenverarbeitung der öffentlichen Stellen** **Erster Unterabschnitt** **Rechtsgrundlagen der Datenverarbeitung**	**Zweiter Abschnitt** **Datenverarbeitung der öffentlichen Stellen** **Erster Unterabschnitt** **Rechtsgrundlagen der Datenverarbeitung**	
§ 12 a.F. Anwendungsbereich	§ 12 n.F. Anwendungsbereich	
(1) Die Vorschriften dieses Abschnittes gelten für öffentliche Stellen des Bundes, soweit sie nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen.	(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 17, 19 und 20 auch für die öffentlichen Stellen der Länder, soweit sie	(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	*Die Änderungen der Verweise in Absatz 2 und 4 sind Folgeänderungen im Zusammenhang mit der Streichung von § 17 a.F., der Schaffung der neuen Vorschrift des § 19 a, der Einbeziehung der Erhebung in § 28 Abs. 1 sowie der Einfügung eines neuen Absatzes 2 in § 28.*
1. Bundesrecht ausführen und nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen oder	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.	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.	(3) Für Landesbeauftragte für den Datenschutz gilt § 23 Abs. 4 entsprechend.	
(4) Werden personenbezogene Daten für frühere, bestehende oder zukünftige dienst- oder arbeitsrechtliche Rechtsver-hältnisse verarbeitet oder genutzt, gelten anstelle der §§ 14 bis 17, 19 und 20 der § 28 Abs. 1 und 2 Nr. 1 sowie die §§ 33 bis 35.	(4) Werden personenbezogene Daten für frühere, bestehende oder zukünftige dienst- oder arbeitsrechtliche Rechtsver-hältnisse erhoben, verarbeitet oder ge-nutzt, gelten anstelle der §§ 13 bis 16, 19 bis 20 der § 28 Abs. 1 und 3 Nr. 1 sowie die §§ 33 bis 35, auch soweit personen-bezogene Daten	*Durch die Ergänzung in Absatz 4 war sicherzustellen, dass Arbeitnehmerdaten unabhängig von dem verwendeten Speichermedium geschützt sind.*

	weder automatisiert verarbeitet noch in nicht automatisierten Dateien verarbeitet oder genutzt oder dafür erhoben werden.	
§ 13 a.F. Datenerhebung	§ 13 n.F. Datenerhebung	
(1) Das Erheben personenbezogener Da-ten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stellen erforderlich ist.	(1) Das Erheben personenbezogener Da-ten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist.	*In Absatz 1 steht die Ersetzung des Begriffs „erhebenden Stellen“ durch den der „verantwortlichen Stelle“ im Zusammenhang mit der Ersetzung des Begriffs der speichernden Stelle durch den der verantwortlichen Stelle (vgl. hierzu die Begründung zu § 3 Abs. 7). Anstelle der bisherigen Pluralform („Stellen“) wurde in Übereinstimmung mit § 14 Abs. 1 die Singularform gewählt. Im Übrigen wird auf die Begründung zu § 4 ver-wiesen.*
	(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.	***Folgeänderung (Beschränkung der Hinweispflicht auf den öffentlichen Bereich durch Einstellung der Vorschrift des § 4 Abs. 4 in § 13).***
(2) [1]Personenbezogene Daten sind beim Betroffenen zu erheben. [2]Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn	(2) Das Erheben besonderer Arten personenbezogener Daten (§ 3 Abs. 9) ist nur zulässig, soweit	*Absatz 2 setzt Artikel 8 der Richtlinie um, der ein generelles Verwendungsverbot mit enumerativen Ausnahmetatbeständen für die in § 3 Abs. 9 bezeichneten Daten vor-sieht. Durch die Nummern 1 bis 9 werden die nach der Richtlinie möglichen Ausnah-men im Hinblick auf das Bestimmtheitsgebot konkretisiert. Aufgrund der Subsidiarität des Bundesdatenschutzgesetzes nach § 1 Abs. 3 gelten die Einschränkungen des Ab-satzes 2 nur für Bereiche, in denen spezialgesetzliche Regelungen für die Verwendung der in § 3 Abs. 9 genannten Arten von Daten fehlen. Dies gilt etwa für die Datenschutz-regelungen im Bereich des Gesundheitswesens, die von Artikel 8 Abs. 3 der Richtlinie erfasst werden. Ferner geht die Gesetzgebung auf dem Gebiet der sozialen Sicherheit den hier geschaffenen Regelungen vor, da es sich dabei um ein „wichtiges öffentliches Interesse“ im Sinne von Artikel 8 Abs. 4 der Richtlinie handelt, bei dessen Vorliegen Ausnahmen von dem Verwendungsverbot des Absatzes 1 zulässig sind. Dies wird im Erwägungsgrund 34 der Richtlinie besonders hervorgehoben. In Erwägungsgrund 35 wird darüber hinaus ausgeführt, dass die Verarbeitung personenbezogener Daten durch staatliche Stellen für verfassungsrechtlich oder im Völkerrecht niedergelegte Zwecke von staatlich anerkannten Religionsgesellschaften im Hinblick auf ein wichtiges öffentliches Interesse erfolgt.*
1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder	1. eine Rechtsvorschrift dies vorsieht oder aus Gründen eines wichtigen öffentlichen Interesses zwingend erfordert,	*Absatz 2 Nr. 1 verdeutlicht, dass die Erhebung der in § 3 Abs. 9 genannten Arten von Daten aufgrund entsprechender bereichspezifischer Ermächtigungsgrundlagen oder dann zulässig ist, wenn die Erhebung zur Ermittlung des Sachverhalts zu einem auf sol-che Daten bezogenen Tatbestandsmerkmal einer bereichspezifischen Norm aus Grün-den eines wichtigen öffentlichen Interesses zwingend erforderlich ist.*

2. a) die zu erfüllende Verwaltungsaufgabe ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder b) die Erhebung beim Betroffenen ei-nen unverhältnismäßigen Aufwand erfordern würde und keine Anhalts-punkte dafür bestehen, daß über-wiegende schutzwürdige Interessen der Betroffenen beeinträchtigt wer-den.	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,	*Nummern 2, 3 und 4 setzen Artikel 8 Abs. 2 Buchstaben a, c und e der Richtlinie um.*
	5. dies zur Abwehr einer erhelbichen 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,	*Die Nummern 5 und 6 beruhen auf einer Umsetzung des Artikels 8 Abs. 4 der Richtli-nie. Die Anwendbarkeit der Nummer 6 setzt in Anbetracht der Anforderungen des Arti-kels 8 Abs. 4 der Richtlinie voraus, dass die Schwelle für die Annahme erheblicher Nachteile oder erheblicher Belange des Gemeinwohls hoch ist. Nicht jedes öffentliche Interesse ist ausreichend.*
	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 entsprechen-den Geheimhaltungspflicht unterliegen,	*Nummer 7 setzt Artikel 8 Abs. 3 der Richtlinie um und schafft eine gesetzliche Grundlage für die Erhebung von Daten, um die Notwendigkeit der Einwilligung verbunden mit der Beachtung des Ausdrücklichkeitserfordernisses nach § 4 a Abs. 3 zu vermeiden. Für die Verarbeitung und Nutzung der Daten sind wie bisher gemäß § 1 Abs. 3 Satz 2 Berufs- und besondere Amtsgeheimnisse maßgeblich, die ein solches Ausdrücklichkeitserfordernis nicht kennen. Die Vorschrift erfasst auch die für die medizinische Begutachtung erforderliche Diagnostik. Die Verwaltung von Gesundheitsdiensten umfasst auch die Abrechnung ihrer Leistungen.*
	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	*Im Rahmen der Nummer 8 kommt bei der Abwägung und Gewichtung zwischen dem wissenschaftlichen Interesse an dem Forschungsvorhaben und dem Individualinteresse des Betroffenen am Ausschluss der Erhebung seiner Daten dem öffentlichen Interesse an dem Forschungsvorhaben eine erhebliche Bedeutung zu. Die grundgesetzlich geschützte zweckfreie wissenschaftliche Forschung liegt regelmäßig im öffentlichen Interesse, wie es Artikel 8 Abs. 4 der Richtlinie fordert.*

	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.	*Nummer 9 schafft eine Ausnahme außerhalb des von dem Anwendungsbereich der Richtlinie betroffenen Gegenstands der ersten Säule des EU-Vertrages.*
(3) [1]Werden personenbezogene Daten beim Betroffenen mit seiner Kenntnis er-hoben, so ist der Erhebungszweck ihm ge-genüber anzugeben. [2]Werden sie beim Betroffenen aufgrund einer Rechtsvor-schrift erhoben, die zur Auskunft verpflich-tet, oder ist die Erteilung der Auskunft Vor-aussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hier-auf, sonst auf die Freiwilligkeit seiner An-gaben hinzuweisen. [3]Auf Verlangen ist er über die Rechtsvorschrift und über die Fol-gen der Verweigerung von Angaben aufzu-klären.		
(4) Werden personenbezogene Daten statt beim Betroffenen bei einer nicht-öffentli-chen Stelle erhoben, so ist die Stelle auf die Rechtsvorschrift, die zur Auskunft ver-pflichtet, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen.		
§ 14 a.F.	§ 14 n.F.	
Datenspeicherung, -veränderung und -nut-zung	Datenspeicherung, -veränderung und -nut-zung	
(1) [1]Das Speichern, Verändern oder Nut-zen personenbezogener Daten ist zulässig, wenn es zur Erfüllung der in der Zustän-digkeit der speichernden Stelle liegenden Aufgaben erforderlich ist und es für die Zwe-cke erfolgt, für die die Daten erhoben wor-den sind. [2]Ist keine Erhebung voraus-gegangen, dürfen die Daten nur für die Zwe-	(1) [1]Das Speichern, Verändern oder Nut-zen personenbezogener Daten ist zulässig, wenn es zur Erfüllung der in der Zustän-digkeit der verantwortlichen Stelle liegen-den Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die Daten erho-ben worden sind. [2]Ist keine Erhebung vor-ausgegangen, dürfen die Daten nur für die	*Die Änderungen sind Folgeänderungen im Zusammenhang mit der Ersetzung des Begriffs der speichernden Stelle durch den der verantwortlichen Stelle (vgl. hierzu die Begründung zu § 3 Abs. 7).*

cke geändert oder genutzt werden, für die sie gespeichert worden sind.	Zwecke geändert oder genutzt werden, für die sie gespeichert worden sind.	
(2) Das Speichern, Verändern oder Nutzen für andere Zwecke ist nur zulässig, wenn	(2) Das Speichern, Verändern oder Nutzen für andere Zwecke ist nur zulässig, wenn	
1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,	1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,	
2. der Betroffene eingewilligt hat,	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,	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,	4. Angaben des Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,	
5. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die speichernde Stelle sie veröffentlichen dürfte, es sei denn, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Zweckänderung offensichtlich überwiegt,	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 Zweck-änderung offensichtlich überwiegt,	***Folgeänderung zu*** [§ 10 Abs. 5] ***(Vereinheitlichung des Sprachgebrauchs durch Ersetzung von „allgemein zugänglichen Quellen“ durch „allgemein zugänglich“).***
6. es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit erforderlich ist,	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,	*In Absatz 2 Nr. 6 bedurfte es zur Vermeidung von Wertungswidersprüchen einer entsprechenden Ergänzung für Daten, die nicht § 3 Abs. 9 unterfallen, da § 13 Abs. 2 Nr. 6 die Erhebung von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) auch zur Wahrung erheblicher Belange des Gemeinwohls vorsieht. Die Wörter „sonst unmittelbar drohenden“ wurden in Anpassung an die gebräuchliche Terminologie in bereichsspezifischen Gesetzen gestrichen.*
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 Strafgesetzbuches oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung	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 Strafgesetzbuches oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung	

von Bußgeldentscheidungen erforder-lich ist,	von Bußgeldentscheidungen erforder-lich ist,	
8. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder	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 For-schung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.	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 For-schung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.	
(3) [1]Eine Verarbeitung oder Nutzung für andere Zwecke liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprü-fung oder der Durchführung von Organisationsuntersuchungen für die speichernde Stelle dient. [2]Das gilt auch für die Verarbeitung oder Nutzung zu Ausbildungs- und Prüfungszwecken durch die speichernde Stelle, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.	(3) [1]Eine Verarbeitung oder Nutzung für andere Zwecke liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprü-fung oder der Durchführung von Organisationsuntersuchungen für die verantwortli-che Stelle dient. [2]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.	(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) [1]Das Speichern, Verändern oder Nutzen von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) für andere Zwecke ist nur zulässig, wenn	*In Absatz 5 bedurfte es auf Grund der Regelung der Erhebung besonderer Arten personenbezogener Daten (§ 3 Abs. 9) in Verbindung mit § 13 Abs. 2 einer Bestimmung zur weiteren zweckändernden Verwendung dieser Daten.*

	1. die Voraussetzungen vorliegen, die ei-ne Erhebung nach § 13 Abs. 2 Nr. 1 bis 6 oder 9 zulassen würden oder	*Durch Verweis auf die Voraussetzungen des § 13 Abs. 2 in Nummer 1 wird sichergestellt, dass sich die zweckändernde Verwendung in Übereinstimmung mit Artikel 6 Abs. 1 Buchstabe b der Richtlinie und ebenfalls im Rahmen der Möglichkeiten des Artikels 8 der Richtlinie bewegt.*
	2. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das öffentliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht wer-den kann.	*Im Rahmen der Durchführung von Forschungsvorhaben ist zunächst wichtige Aufgabe des Wissenschaftlers, Ziel und Zweck des jeweiligen Forschungsvorhabens zu umschreiben. Dies hat in einer Weise zu erfolgen, die es ermöglicht, weitere Änderungen der wissenschaftlichen Fragestellung von vornherein mit einzubeziehen, so dass inso-weit keine Zweckänderungen im Sinne der Nummer 2 vorliegen. Das in Nummer 2 sta-tuierte Abwägungserfordernis des öffentlichen Interesses an der Durchführung des Forschungsvorhabens mit dem Interesse des Betroffenen an dem Ausschluss der Zweckänderung ist somit erst dann zu prüfen, wenn es sich um Änderungen außerhalb der oben beschriebenen wissenschaftlichen Fragestellung handelt. Zudem stellt Satz 2 sicher, dass dem wissenschaftlichen Interesse an dem Forschungsvorhaben im Rah-men dieser Abwägung besonderes Gewicht zukommt.*
	[2]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.	*Für die Speicherung, Veränderung oder Nutzung dieser Daten sind gemäß § 1 Abs. 3 Satz 2 wie bisher Berufs- und besondere Amtsgeheimnisse maßgeblich, die das Ausdrücklichkeitserfordernis des § 4 a Abs. 3 nicht kennen. Der Gedanke des Absatzes 6 findet über die in § 15 Abs. 1 Nr. 2 und § 16 Abs. 1 Nr. 1 erfolgende Bezugnahme auf § 14 auch Eingang in die für die Übermittlung geltenden Vorschriften*
§ 15 a.F.	§ 15 n.F.	
Datenübermittlung an öffentliche Stellen	Datenübermittlung an öffentliche Stellen	
(1) Die Übermittlung personenbezogener Daten an öffentliche Stellen ist zulässig, wenn	(1) Die Übermittlung personenbezogener Daten an öffentliche Stellen ist zulässig, wenn	*Die Vorschrift regelt den Fall der Übermittlung von Daten an öffentliche Stellen. Wesentliches Element der Übermittlung ist die Bekanntgabe von Daten an Dritte (§ 3 Abs. 4 Nr. 3). Zu den datenempfangenden öffentlichen Stellen im Sinne der Vorschrift zählen alle deutschen öffentlichen Stellen, soweit sie Dritte sind, sowie solche im EU-Ausland. Um Missverständnisse mit dem weitergehenden Begriff des nun in § 3 Abs. 8 Satz 1 definierten Empfängers zu vermeiden, war der Begriff des Empfängers durch den des Dritten, an den die Daten übermittelt werden, zu ersetzen bzw. die Vorschrift entsprechend zu modifizieren.*
1. sie zur Erfüllung der in der Zuständig-keit der übermittelnden Stelle oder des Empfängers liegenden Aufgaben erforderlich ist und	1. sie zur Erfüllung der in der Zuständig-keit der übermittelnden Stelle oder des Dritten, an den die Daten übermittelt werden, liegenden Aufgaben erforder-lich ist	

2. die Voraussetzungen vorliegen, die eine Nutzung nach § 14 zulassen wür-den.	und 2. die Voraussetzungen vorliegen, die ei-ne Nutzung nach § 14 zulassen wür-den.	
(2) [1]Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. [2]Erfolgt die Übermittlung auf Ersuchen des Empfängers, trägt dieser die Verantwortung. [3]In diesem Falle prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Empfängers liegt, es sei denn, daß besonderer Anlaß zur Prüfung der Zulässigkeit der Übermittlung besteht. [4]§ 10 Abs. 4 bleibt unberührt.	(2) [1]Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. [2]Erfolgt die Übermittlung auf Ersuchen des Dritten, an den die Daten übermittelt werden, trägt dieser die Verantwor-tung. [3]In diesem Falle 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. [4]§ 10 Abs. 4 bleibt unberührt.	
(3) [1]Der Empfänger darf die übermittelten Daten für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. [2]Eine Verarbeitung oder Nutzung für andere Zwecke ist nur unter den Voraussetzungen des § 14 Abs. 2 zulässig.	(3) [1]Der Dritte, an den die Daten übermittelt werden, darf diese für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. [2]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 dem Empfänger ausreichende Datenschutzmaßnahmen getroffen werden.	(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 dür-fen, weitere personenbezogene Daten des Betroffenen oder eines Dritten in Akten so verbunden, daß eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, so ist die Übermittlung auch dieser Da-ten zulässig, soweit nicht berechtigte Interessen des Betroffenen oder eines Dritten an deren Geheimhaltung offensichtlich ü-	(5) Sind mit personenbezogenen Daten, die nach Absatz 1 übermittelt werden dür-fen, weitere personenbezogene Daten des Betroffenen oder eines Dritten so verbun-den, dass eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zuläs-sig, soweit nicht berechtigte Interessen des Betroffenen oder eines Dritten an deren Geheimhaltung offensichtlich überwiegen;	*Hinsichtlich des Verzichts auf den Begriff „Akten“ in Absatz 5 wird auf die Begründung zu § 3 Abs. 2 verwiesen.*

berwiegen; eine Nutzung dieser Daten ist unzulässig.	eine Nutzung dieser Daten ist unzulässig.	
(6) Absatz 5 gilt entsprechend, wenn personenbezogene Daten innerhalb einer öffentlichen Stelle weitergegeben werden.	(6) Absatz 5 gilt entsprechend, wenn personenbezogene Daten innerhalb einer öffentlichen Stelle weitergegeben werden.	
§ 16 a.F.	§ 16 n.F.	
Datenübermittlung an nicht-öffentliche Stellen	Datenübermittlung an nicht-öffentliche Stellen	
(1) Die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen ist zulässig, wenn	(1) Die Übermittlung personenbezogener Daten an nicht öffentliche Stellen ist zulässig, wenn	*Zur Ersetzung des Begriffs des Empfängers durch den Begriff des Dritten, an den die Daten übermittelt werden, wird auf die Begründung zu § 15 verwiesen.*
1. sie zur Erfüllung der in der Zuständig-keit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 14 zulassen würden, oder	1. sie zur Erfüllung der in der Zuständig-keit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 14 zulassen würden, oder	
2. der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interes-se an dem Ausschluß der Übermittlung hat.	2. der Dritte, an den die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffe-ne 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.	*Die Ergänzung in Absatz 1 Nr. 2 Satz 2 stellt sicher, dass bei einer Übermittlung von Daten nach § 3 Abs. 9 die Anforderungen des § 14 Abs. 5 und 6 gewahrt werden. Auf die Begründung zu dieser Vorschrift wird verwiesen. Der letzte Halbsatz setzt Artikel 8 Abs. 2 Buchstabe e 2. Halbsatz der Richtlinie um und gewährleistet unter den genannten Voraussetzungen die Übermittlung von Daten nach § 3 Abs. 9 an nicht-öffentliche Stellen.*
(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.	(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.	
(3) [1]In den Fällen der Übermittlung nach Absatz 1 Nr. 2 unterrichtet die übermitteln-	(3) [1]In den Fällen der Übermittlung nach Absatz 1 Nr. 2 unterrichtet die übermitteln-	

de Stelle den Betroffenen von der Übermittlung seiner Daten. [2]Dies gilt nicht, wenn damit zu rechnen ist, daß er davon auf andere Weise Kenntnis erlangt, oder wenn die Unterrichtung die öffentliche Si-cherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde.	de Stelle den Betroffenen von der Übermittlung seiner Daten. [2]Dies gilt nicht, wenn damit zu rechnen ist, dass er davon auf andere Weise Kenntnis erlangt, oder wenn die Unterrichtung die öffentliche Si-cherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde.	
(4) [1]Der Empfänger darf die übermittelten Daten nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. [2]Die übermittelnde Stelle hat den Empfänger darauf hinzuweisen. [3]Eine Verarbeitung oder Nutzung für ande-re Zwecke ist zulässig, wenn eine Über-mittlung nach Absatz 1 zulässig wäre und die übermittelnde Stelle zugestimmt hat.	(4) [1]Der Dritte, an den die Daten übermittelt werden, darf diese nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. [2]Die über-mittelnde Stelle hat ihn darauf hinzuweisen. [3]Eine Verarbeitung oder Nutzung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Absatz 1 zulässig wäre und die übermittelnde Stelle zugestimmt hat.	
§ 17 a.F.	§ 17 n.F.	
Datenübermittlung an Stellen außerhalb des Geltungsbereiches dieses Gesetzes	Datenübermittlung an Stellen außerhalb des Geltungsbereiches dieses Gesetzes	
(1) Für die Übermittlung personenbezogener Daten an Stellen außerhalb des Geltungsbereichs dieses Gesetzes sowie an über- und zwischenstaatliche Stellen gilt § 16 Abs. 1 nach Maßgabe der für diese Übermittlung geltenden Gesetze und Vereinbarungen, sowie § 16 Abs. 3.	Hinweis: Die Vorschrift wurde vollständig aufgehoben.	*Auf die Begründung zu § 4 b wird verwiesen.*
(2) Eine Übermittlung unterbleibt, soweit Grund zu der Annahme besteht, daß durch sie gegen den Zweck eines deutschen Gesetzes verstoßen würde.		
(3) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.		
(4) Der Empfänger ist darauf hinzuweisen, daß die übermittelten Daten nur zu dem Zweck verarbeitet oder genutzt werden dür-		

fen, zu dessen Erfüllung sie ihm über-mittelt werden.		
§ 18 a.F.	§ 18 n.F.	
Durchführung des Datenschutzes in der Bundesverwaltung	Durchführung des Datenschutzes in der Bundesverwaltung	
(1) [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. [2]Das gleiche gilt für die Vorstände der aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange ihnen ein ausschließliches Recht nach dem Postgesetz zusteht.	(1) [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. [2]Das gleiche gilt für die Vorstände der aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange ihnen ein ausschließliches Recht nach dem Postgesetz zusteht.	
(2) [1]Die öffentlichen Stellen führen ein Verzeichnis der eingesetzten Datenverarbeitungsanlagen. [2]Für ihre Dateien haben sie schriftlich festzulegen: 1. Bezeichnung und Art der Dateien, 2. Zweckbestimmung, 3. Art der gespeicherten Daten, 4. betroffenen Personenkreis, 5. Art der regelmäßig zu übermittelnden Daten und deren Empfänger, 6. Regelfristen für die Löschung der Daten, 7. zugriffsberechtigte Personengruppen oder Personen, die allein zugriffsberechtigt sind.	(2) [1]Die öffentlichen Stellen führen ein Verzeichnis der eingesetzten Datenverarbeitungsanlagen. [2]Für ihre automatisierten Verarbeitungen haben sie die Angaben nach § 4e sowie die Rechtsgrundlage der Verarbeitung schriftlich festzulegen. [3]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. [4]Für automatisierte Verarbeitungen, die in gleicher oder ähnlicher Weise mehrfach geführt werden, können die Festlegungen zusammengefasst werden.	*Um unnötige Wiederholungen zu vermeiden, wurde die Auflistung des Absatzes 2 Satz 2 durch den Verweis auf die neue Vorschrift des § 4 e ersetzt. Die Angabe der Rechtsgrundlage der Verarbeitung dient der Erleichterung der Überprüfung durch den Bundesbeauftragten für den Datenschutz.* *Absatz 2 Satz 3 und 4 beinhaltet eine Einschränkung der Verpflichtung der öffentlichen Stellen zur Führung eines Verzeichnisses ihrer automatisierten Verarbeitungen, die der Entlastung dieser Stellen dient. Anwendungsbeispiele sind in erster Linie triviale automatisierte Verarbeitungen (Geburtstagslisten u.ä.).*

[3]Sie haben ferner dafür zu sorgen, daß die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, überwacht wird.		
(3) Absatz 2 Satz 2 gilt nicht für Dateien, die nur vorübergehend vorgehalten und innerhalb von drei Monaten nach ihrer Er-stellung gelöscht werden.		*Die umzusetzende Richtlinie sieht eine Privilegierungsmöglichkeit für nur vorüberge-hend vorgehaltene Dateien im Sinne des § 18 Abs. 3 a.F. nicht vor. Die Vorschrift des Absatzes 3 war daher ersatzlos aufzuheben.*
Zweiter Unterabschnitt **Rechte des Betroffenen**	**Zweiter Unterabschnitt** **Rechte des Betroffenen**	
§ 19 a.F. Auskunft an den Betroffenen	§ 19 n.F. Auskunft an den Betroffenen	
(1) [1]Dem Betroffenen ist auf Antrag Auskunft zu erteilen über	(1) [1]Dem Betroffenen ist auf Antrag Auskunft zu erteilen über	*Durch die Neufassung des Absatzes 1 wird Artikel 12 Buchstabe a, 1. Spiegelstrich der Richtlinie umgesetzt.*
1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf Herkunft oder Empfänger dieser Daten beziehen, und	1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,	*Die Neufassung erweitert den Umfang des Auskunftsrechts um die Information über Empfänger oder Kategorien von Empfängern. Um inhaltliche Überschneidungen von Nummer 2 mit Nummer 1 a.F. zu vermeiden, war Nummer 1 a.F. entsprechend zu modifizieren. Im Hinblick auf den Begriff des Empfängers wird auf § 3 Abs. 8 Satz 1 sowie die Begründung hierzu verwiesen.*
2. den Zweck der Speicherung.	2. die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden, und 3. den Zweck der Speicherung.	*Die Änderungen in Absatz 1 Satz 4, Absatz 4 und 6 sind Folgeänderungen im Zusammenhang mit der Ersetzung des Begriffs der speichernden Stelle durch den der verantwortlichen Stelle (vgl. hierzu die Begründung zu § 3 Abs. 7). Hinsichtlich der Ersetzung des Wortes „Akten“ durch die Wörter „weder automatisiert noch in nicht-automatisier-ten Dateien“ in Absatz 1 Satz 3 wird auf die Begründung zu § 3 Abs. 2 verwiesen.*
[2]In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. [3]Sind die personenbezogenen Daten in Akten 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 au-ßer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht. [4]Die speichernde Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Er-	[2]In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. [3]Sind die personenbezogenen Daten we-der automatisiert noch in nicht automatisierten Dateien gespeichert, wird die Auskunft nur erteilt, soweit der Betroffene An-gaben macht, die das Auffinden der Da-ten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend	

messen.	gemachten Informationsinteresse steht. [4]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 wer-den dürfen, oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen.	(2) Absatz 1 gilt nicht für personenbezogene Daten, die nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht wer-den dürfen, oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen und eine Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.	*Die Ausnahme des Absatzes 2 Satz 1 wurde in Anwendung des Artikels 13 Abs. 1 Buchstabe g der Richtlinie modifiziert.*
(3) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Da-ten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militäri-schen Abschirmdienst und, soweit die Si-cherheit des Bundes berührt wird, andere Behörden des Bundesministers der Vertei-digung, ist sie nur mit Zustimmung dieser Stellen zulässig.	(3) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Da-ten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militäri-schen Abschirmdienst und, soweit die Si-cherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.	*Die Änderung in Absatz 3 geht auf einen Beschluss des Bundeskabinetts vom 20. Januar 1993 (GMBl. S. 46) zurück, nach dem einheitlich für alle Bundesressorts die sächliche Bezeichnungsform einzuführen ist. Entsprechende Änderungen finden sich in §§ 22 Abs. 5 und 23 Abs. 3 und 5.*
(4) Die Auskunftserteilung unterbleibt, soweit	(4) Die Auskunftserteilung unterbleibt, soweit	
1. die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufga-ben gefährden würde,	1. die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufga-ben gefährden würde,	
2. die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder	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	3. die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten	

Interessen eines Dritten, geheimgehalten werden müssen	Interessen eines Dritten, geheimgehalten werden müssen	
und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muß.	und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.	
(5) [1]Die Ablehnung der Auskunftserteilung bedarf einer Begründung nicht, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entschei-dung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. [2]In diesem Falle ist der Betroffene darauf hinzuweisen, daß er sich an den Bundesbeauftragten für den Datenschutz wenden kann.	(5) [1]Die Ablehnung der Auskunftserteilung bedarf einer Begründung nicht, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entschei-dung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. [2]In diesem Falle ist der Betroffene darauf hinzuweisen, dass er sich an den Bundesbeauftragten für den Datenschutz wenden kann.	
(6) [1]Wird dem Betroffenen keine Auskunft erteilt, so ist sie auf sein Verlangen dem Bundesbeauftragten für den Datenschutz zu erteilen, soweit nicht die jeweils zustän-dige oberste Bundesbehörde im Einzelfall feststellt, daß dadurch die Sicherheit des Bundes oder eines Landes gefährdet wür-de. [2]Die Mitteilung des Bundesbeauftrag-ten an den Betroffenen darf keine Rück-schlüsse auf den Erkenntnisstand der spei-chernden Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zu-stimmt.	(6) [1]Wird dem Betroffenen keine Auskunft erteilt, so ist sie auf sein Verlangen dem Bundesbeauftragten für den Datenschutz zu erteilen, soweit nicht die jeweils zustän-dige oberste Bundesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. [2]Die Mitteilung des Bundesbeauftrag-ten 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.	(7) Die Auskunft ist unentgeltlich.	
	§ 19a n.F.	
	Benachrichtigung	
	(1) [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. [2]Der Betroffene ist auch	*Absatz 1 führt in Umsetzung von Artikel 11 der Richtlinie eine Benachrichtigungspflicht im öffentlichen Bereich für die Fälle ein, in denen Daten nicht beim Betroffenen unmittelbar selbst erhoben werden.*

	über die Empfänger oder Kategorien von Empfängern von Daten zu unterrichten, soweit er nicht mit der Übermittlung an diese rechnen muss. [3]Sofern eine Übermittlung vorgesehen ist, hat die Unterrichtung spätestens bei der ersten Übermittlung zu erfolgen.	
	(2) [1]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 in Absatz 2 Nr. 1 bis 3 geregelten Ausnahmen von der Benachrichtigungspflicht setzen Artikel 11 Abs. 2 der Richtlinie um; die in Absatz 3 geregelten Ausnahmen be-ruhen auf Artikel 13 der Richtlinie.*
	[2]Die verantwortliche Stelle legt schriftlich fest, unter welchen Voraussetzungen von einer Benachrichtigung nach Nummer 2 oder 3 abgesehen wird.	*Durch Absatz 2 Satz 2 wird das Erfordernis der „geeigneten Garantien“ nach Artikel 11 Abs. 2 Satz 2 der Richtlinie umgesetzt. Der behördliche Beauftragte für den Datenschutz wirkt auf die Einhaltung dieser Vorschrift hin.*
	(3) § 19 Abs. 2 bis 4 gilt entsprechend.	
§ 20 a.F.	§ 20 n.F.	
Berichtigung, Löschung und Sperrung von Daten	Berichtigung, Löschung und Sperrung von Daten; Widerspruchsrecht	*Die Überschrift war aufgrund der Einfügung des Widerspruchsrechts in Absatz 5 zu ergänzen.*
(1) [1]Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. [2]Wird festgestellt, daß personenbezogene Daten in Akten unrichtig sind, oder wird ihre Richtigkeit von dem Betroffenen bestritten, so ist dies in der Akte zu vermerken oder auf sonstige Weise festzuhalten.	(1) [1]Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. [2]Wird festgestellt, dass personenbezogene Daten, die weder automatisiert verarbeitet noch in nicht automatisierten Dateien gespeichert sind, unrichtig sind, oder wird ihre Richtigkeit von dem Betroffenen be-stritten, so ist dies in geeigneter Weise festzuhalten.	*Hinsichtlich der Ersetzung des Wortes „Akten“ durch die Wörter „weder automatisiert verarbeitet noch in nicht-automatisierten Dateien gespeichert“ wird auf die Begründung zu § 3 Abs. 2 verwiesen. Die Änderungen im zweiten Teil von Satz 2 sind bloße Folgeänderungen ohne inhaltliche Auswirkung.*
(2) Personenbezogene Daten in Dateien	(2) Personenbezogene Daten, die automa-	*Hinsichtlich der Änderung in Satz 1 vor Nr. 1 wird auf die Begründung zu § 3 Abs. 2 ver-*

sind zu löschen, wenn 1. ihre Speicherung unzulässig ist oder 2. ihre Kenntnis für die speichernde Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.	tisiert 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.	*wiesen. Die Änderung in Absatz 2 Nr. 2 ist eine Folgeänderung im Zusammenhang mit der Ersetzung des Begriffs der speichernden Stelle durch den der verantwortlichen Stelle (vgl. hierzu die Begründung zu § 3 Abs. 7).*
(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.	(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 in Dateien sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrich-tigkeit feststellen läßt.	(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.	*Auf die Begründung zu § 3 Abs. 2 wird verwiesen.*
(5) Personenbezogene Daten in Akten 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.	(5) [1]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	*Absatz 5 setzt Artikel 14 Buchstabe a der Richtlinie für den öffentlichen Bereich um. Ausweislich des Erwägungsgrundes 45 der Richtlinie gilt das Widerspruchsrecht des Betroffenen für Fälle rechtmäßiger Datenverarbeitung. Begründet ist der Widerspruch des Betroffenen allerdings nur, sofern besondere Umstände in der Person des Betroffe-nen vorliegen und das schutzwürdige Interesse des Betroffenen an der Unterlassung das der speichernden Stelle an der Verarbeitung überwiegt. Diese Voraussetzungen werden nur in Ausnahmefällen erfüllt sein. Vor dem Hintergrund, dass dem Wider-spruch eine rechtmäßige Verarbeitung und Nutzung zugrunde liegt, ist bei der Prüfung des Vorliegens einer besonderen persönlichen Situation, die das öffentliche Interesse an der Verarbeitung und*

	Interesse der verantwortlichen Stelle an dieser Erhebung, Verarbeitung oder Nutzung überwiegt. [2]Satz 1 gilt nicht, wenn eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung verpflichtet.	*Nutzung zurücktreten lässt, ein besonders strenger Maßstab anzulegen. Beispiele für derartige Regelungen finden sich bereits im Melderecht (§ 7 Nr. 5 Melderechtsrahmengesetz), im Sozialgesetzbuch (§ 76 Abs. 2 Nr. 1 SGB X) und im Krebsregistergesetz (§ 3 Abs. 2 Satz 2). Satz 2 schließt das Widerspruchsrecht in den Fällen aus, in denen eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nut-zung verpflichtet. Dies steht im Einklang mit der Richtlinie, da Artikel 14 Buchstabe a der Richtlinie nicht auf Artikel 7 Buchstabe c der Richtlinie verweist.* *Zusätzliche bereichsspezifische Ausnahmen sind möglich (Artikel 14 Buchstabe a, zweiter Halbsatz der Richtlinie).*
(6) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn 1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweis-not oder aus sonstigen im überwiegen-den Interesse der speichernden Stelle oder eines Dritten liegenden Gründen unerläßlich ist und 2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.	(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 Sper-rung schutzwürdige Interessen des Betrof-fenen beeinträchtigt würden und die Daten für die Aufgabenerfüllung der Behörde nicht mehr erforderlich sind.	*Hinsichtlich der Ersetzung des Wortes „Akten“ durch die Wörter „weder automatisiert verarbeitet noch in einer nicht-automatisierten Datei gespeichert“ wird auf die Begründung zu § 3 Abs. 2 verwiesen.*
(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 regelmäßigen Datenübermittlung diese Da-ten zur Speicherung weitergegeben wer-den, wenn dies zur Wahrung schutzwürdi-ger Interessen des Betroffenen erforderlich ist.	(7) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn 1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweis-not oder aus sonstigen im überwiegen-den 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	*Die Änderung in Absatz 7 Nr. 1 ist eine Folgeänderung im Zusammenhang mit der Ersetzung des Begriffs der speichernden Stelle durch den der verantwortlichen Stelle (vgl. hierzu die Begründung zu § 3 Abs. 7).*
(8) § 2 Abs. 1 bis 6, 8 und 9 des Bundesarchivgesetzes ist anzuwenden.	(8) Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu	*Durch den Wegfall der Regelmäßigkeit der Datenübermittlung als Voraussetzung der Nachberichtspflicht (vgl. § 20 Abs. 7 a.F.) wird in Umsetzung von Artikel 12 Buchstabe c der Richtlinie der Anwendungsbereich der Nachberichtspflicht erweitert. Gleich-zeitig wird - ebenfalls in Umsetzung der Richtlinie - sichergestellt, dass die Nachberichtspflicht*

	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.	*nur besteht, wenn sie keinen unverhältnismäßigen Aufwand erfordert. Durch die Formulierung „und schutzwürdige Interessen des Betroffenen nicht entgegen-stehen“ soll verhindert werden, dass eine Benachrichtigung zu Lasten des Betroffenen erfolgen kann.*
§ 21 a.F.	§ 21 n.F.	
Anrufung des Bundesbeauftragten für den Datenschutz	Anrufung des Bundesbeauftragten für den Datenschutz	
[1]Jedermann kann sich an den Bundesbeauftragten für den Datenschutz wenden, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch öffentliche Stellen des Bundes in seinen Rechten verletzt worden zu sein. [2]Für die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch Gerichte des Bundes gilt dies nur, soweit diese in Verwaltungsangelegenheiten tätig werden.	[1]Jedermann kann sich an den Bundesbeauftragten für den Datenschutz wenden, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch öffentliche Stellen des Bundes in seinen Rechten verletzt worden zu sein. [2]Für die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch Gerichte des Bundes gilt dies nur, soweit diese in Verwaltungsangelegenheiten tätig werden.	
Dritter Unterabschnitt	**Dritter Unterabschnitt**	
Bundesbeauftragter für den Datenschutz	**Bundesbeauftragter für den Datenschutz**	
§ 22 a.F.	§ 22 n.F.	
Wahl des Bundesbeauftragten für den Datenschutz	Wahl des Bundesbeauftragten für den Datenschutz	
(1) [1]Der Deutsche Bundestag wählt auf Vorschlag der Bundesregierung den Bundesbeauftragten für den Datenschutz mit mehr als der Hälfte der gesetzlichen Zahl seiner Mitglieder. [2]Der Bundesbeauftragte muß bei seiner Wahl das 35. Lebensjahr vollendet haben. [3]Der Gewählte ist vom Bundespräsidenten zu ernennen.	(1) [1]Der Deutsche Bundestag wählt auf Vorschlag der Bundesregierung den Bundesbeauftragten für den Datenschutz mit mehr als der Hälfte der gesetzlichen Zahl seiner Mitglieder. [2]Der Bundesbeauftragte muss bei seiner Wahl das 35. Lebensjahr vollendet haben. [3]Der Gewählte ist vom Bundespräsidenten zu ernennen.	

(2) [1]Der Beauftragte leistet vor dem Bundesminister des Innern folgenden Eid:	(2) [1]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.“	"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."	
[2]Der Eid kann auch ohne religiöse Beteuerung geleistet werden.	[2]Der Eid kann auch ohne religiöse Beteuerung geleistet werden.	
(3) [1]Die Amtszeit des Bundesbeauftragten beträgt fünf Jahre. [2]Einmalige Wiederwahl ist zulässig.	(3) [1]Die Amtszeit des Bundesbeauftragten beträgt fünf Jahre. [2]Einmalige Wiederwahl ist zulässig.	
(4) [1]Der Bundesbeauftragte steht nach Maßgabe dieses Gesetzes zum Bund in einem öffentlich-rechtlichen Amtsverhält-nis. [2]Er ist in Ausübung seines Amtes unabhängig und nur dem Gesetz unterwor-fen. [3]Er untersteht der Rechtsaufsicht der Bundesregierung.	(4) [1]Der Bundesbeauftragte steht nach Maßgabe dieses Gesetzes zum Bund in einem öffentlich-rechtlichen Amtsverhält-nis. [2]Er ist in Ausübung seines Amtes unabhängig und nur dem Gesetz unterwor-fen. [3]Er untersteht der Rechtsaufsicht der Bundesregierung.	
(5) [1]Der Bundesbeauftragte wird beim Bundesminister des Innern eingerichtet. [2]Er untersteht der Dienstaufsicht des Bundesministers des Innern. [3]Dem Bundesbeauftragten ist die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen; sie ist im Einzelplan des Bundesministers des Innern in einem eigenen Kapitel auszuweisen. [4]Die Stellen sind im Einvernehmen mit	(5) [1]Der Bundesbeauftragte wird beim Bundesministerium des Innern eingerich-tet. [2]Er untersteht der Dienstaufsicht des Bundesministeriums des Innern. [3]Dem Bundesbeauftragten ist die für die Erfüllung seiner Aufgaben notwendige Perso-nal- und Sachausstattung zur Verfügung zu stellen; sie ist im Einzelplan des Bundesministeriums des Innern in einem eigenen Kapitel auszuweisen. [4]Die Stellen sind	*Zu den Änderungen in Absatz 5 wird auf die Begründung zu § 19 Abs. 3 verwiesen. Wegen der Bedeutung der Vereidigung und der Beauftragung eines Stellvertreters des Bundesbeauftragten bleiben Absatz 2 und 6 insoweit unverändert.*

dem Bundesbeauftragten zu besetzen. [5]Die Mitarbeiter können, falls sie mit der beabsichtigten Maßnahme nicht einver-standen sind, nur im Einvernehmen mit ihm versetzt, abgeordnet oder umgesetzt werden.

(6) [1]Ist der Bundesbeauftragte vorübergehend an der Ausübung seines Amtes verhindert, kann der Bundesminister des Innern einen Vertreter mit der Wahrneh-mung der Geschäfte beauftragen. [2]Der Bundesbeauftragte soll dazu gehört wer-den.

§ 23 a.F.

Rechtsstellung des Bundesbeauftragten für den Datenschutz

(1) [1]Das Amtsverhältnis des Bundesbeauftragten für den Datenschutz beginnt mit der Aushändigung der Ernennungsurkun-de. [2]Es endet

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

[3]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. [4]Im Falle der Beendi-gung des Amtsverhältnisses erhält der Bundesbeauftragte eine vom Bundesprä-sidenten vollzogene Urkunde. [5]Eine Ent-lassung wird mit der Aushändigung der Urkunde wirksam. [6]Auf Ersuchen des Bun-desministers des Innern ist der Bundesbe-auftragte verpflichtet, die Geschäfte bis zur Ernennung seines Nachfolgers weiter-zuführen.

im Einvernehmen mit dem Bundesbeauftragten zu besetzen. [5]Die Mitarbeiter können, falls sie mit der beabsichtigten Maßnahme nicht einverstanden sind, nur im Einvernehmen mit ihm versetzt, abgeord-net oder umgesetzt werden.

(6) [1]Ist der Bundesbeauftragte vorübergehend an der Ausübung seines Amtes verhindert, kann der Bundesminister des Innern einen Vertreter mit der Wahrneh-mung der Geschäfte beauftragen. [2]Der Bundesbeauftragte soll dazu gehört wer-den.

§ 23 n.F.

Rechtsstellung des Bundesbeauftragten für den Datenschutz

(1) [1]Das Amtsverhältnis des Bundesbeauftragten für den Datenschutz beginnt mit der Aushändigung der Ernennungsurkun-de. [2]Es endet

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

[3]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. [4]Im Falle der Beendigung des Amtsverhältnisses erhält der Bundesbeauftragte eine vom Bundespräsidenten vollzogene Urkunde. [5]Eine Entlassung wird mit der Aushändigung der Urkunde wirksam. [6]Auf Ersuchen des Bundesministers des Innern ist der Bundesbeauftragte verpflichtet, die Geschäfte bis zur Ernennung seines Nachfolgers weiter-zuführen.

(2) [1]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 ei-ner Regierung oder einer gesetzgebenden Körperschaft des Bundes oder eines Lan-des angehören. [2]Er darf nicht gegen Ent-gelt außergerichtliche Gutachten abgeben.	(2) [1]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 ei-ner Regierung oder einer gesetzgebenden Körperschaft des Bundes oder eines Lan-des angehören. [2]Er darf nicht gegen Ent-gelt außergerichtliche Gutachten abgeben.	
(3) [1]Der Bundesbeauftragte hat dem Bundesminister des Innern Mitteilung über Geschenke zu machen, die er in bezug auf sein Amt erhält. [2]Der Bundesminister des Innern entscheidet über die Verwendung der Geschenke.	(3) [1]Der Bundesbeauftragte hat dem Bundesministerium des Innern Mitteilung über Geschenke zu machen, die er in bezug auf sein Amt erhält. [2]Das Bundesministerium des Innern entscheidet über die Verwendung der Geschenke.	*Zu den Änderungen in Absatz 3 und Absatz 5 Satz 3 wird auf die Begründung zu § 19 Abs. 3 verwiesen. Wegen der Bedeutung des Amtes des Bundesbeauftragten bleibt Absatz 1 Satz 6 unverändert.*
(4) [1]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. [2]Dies gilt auch für die Mitarbeiter des Bundesbeauftragten mit der Maßgabe, daß über die Ausübung dieses Rechts der Bundesbeauftragte entscheidet. [3]Soweit das Zeugnisverweigerungsrecht des Bundesbeauftragten reicht, darf die Vorlegung oder Auslieferung von Akten oder anderen Schriftstücken von ihm nicht gefordert werden.	(4) [1]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. [2]Dies gilt auch für die Mitarbeiter des Bundesbeauftragten mit der Maßgabe, dass über die Ausübung dieses Rechts der Bundesbeauftragte entscheidet. [3]Soweit das Zeugnisverweigerungsrecht des Bundesbeauftragten reicht, darf die Vorlegung oder Auslieferung von Akten oder anderen Schriftstücken von ihm nicht gefordert werden.	
(5) [1]Der Bundesbeauftragte ist, auch nach Beendigung seines Amtsverhältnisses, verpflichtet, über die ihm amtlich bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren. [2]Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. [3]Der Bundesbeauftragte darf,	(5) [1]Der Bundesbeauftragte ist, auch nach Beendigung seines Amtsverhältnisses, verpflichtet, über die ihm amtlich bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren. [2]Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. [3]Der Bundesbeauftragte darf,	*Die Regelung des Absatzes 5 Satz 5, die an § 27 Abs. 2 BImSchG angelehnt ist, stellt sicher, dass die in den benannten Vorschriften der Abgabenordnung normierten Mitteilungspflichten nicht gelten. Die erfolgte Ergänzung stellt eine Konkretisierung des bereits nach geltendem Recht bestehenden Gebots der Verschwiegenheit für den Bundesbeauftragten für den Datenschutz dar, wonach die ihm bekannt gewordenen Daten grundsätzlich einem Übermittlungsverbot unterliegen, soweit nicht die Ausnahmen der Sätze 2 oder 4 einschlägig sind. Satz 6 sieht – ebenfalls in Anlehnung an § 27 Abs. 2 BImSchG – Ausnahmen von diesem Grundsatz vor. Satz 7 beinhaltet in Umsetzung von Artikel 28 Abs. 3, 3. Spiegelstrich der Richtlinie eine Anzeigebefugnis des Bundes-*

auch wenn er nicht mehr im Amt ist, über solche Angelegenheiten ohne Genehmigung des Bundesministers des Innern weder vor Gericht noch außergerichtlich aussagen oder Erklärungen abgeben. [4]Unberührt bleibt die gesetzlich begründete Pflicht, Straftaten anzuzeigen und bei Gefährdung der freiheitlichen demokratischen Grundordnung für deren Erhaltung einzutreten.	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. [4]Unberührt bleibt die gesetzlich begründe-te Pflicht, Straftaten anzuzeigen und bei Gefährdung der freiheitlichen demokrati-schen Grundordnung für deren Erhaltung einzutreten. [5]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. [6]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. [7]Stellt der Bundesbeauftragte einen Datenschutzverstoß fest, ist er befugt, diesen anzuzeigen und den Betroffenen hierüber zu informieren.	*beauftragten für den Datenschutz sowie dessen Recht, Betroffene zu informieren.*
(6) [1]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. [2]Die Genehmigung, ein Gutachten zu erstatten, kann versagt werden, wenn die Erstattung den dienstlichen Interessen Nachteile bereiten würde. [3]§ 28 des Gesetzes über das Bundesverfassungsgericht in der Fassung der Bekanntmachung vom 12. Dezember 1985 (BGBl. I S. 2229) bleibt unberührt.	(6) [1]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. [2]Die Genehmigung, ein Gutachten zu erstatten, kann versagt werden, wenn die Erstattung den dienstlichen Interessen Nachteile bereiten würde. [3]§ 28 des Bundesverfassungsgerichtsgesetzes bleibt unberührt.	

(7) [1]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 Absat-zes 1 Satz 6 bis zum Ende des Monats, in dem die Geschäftsführung endet, Amtsbe-züge in Höhe der einem Bundesbeamten der Besoldungsgruppe B 9 zustehenden Besoldung. [2]Das Bundesreisekostengesetz und das Bundesumzugskostengesetz sind entsprechend anzuwenden. [3]Im übrigen sind die §§ 13 bis 20 des Bundesministergesetzes in der Fassung der Bekanntmachung vom 27. Juli 1971 (BGBl. I S. 1166), zuletzt geändert durch das Ge-setz zur Kürzung des Amtsgehalts der Mit-glieder der Bundesregierung und der Parlamentarischen Staatssekretäre vom 22. Dezember 1982 (BGBl. I S. 2007), mit der Maßgabe anzuwenden, daß an die Stelle der zweijährigen Amtszeit in § 15 Abs. 1 des Bundesministergesetzes eine Amtszeit von fünf Jahren tritt. [4]Abweichend von Satz 3 in Verbindung mit den §§ 15 bis 17 des Bundesministergesetzes berechnet sich das Ruhegehalt des Bundesbeauftrag-ten unter Hinzurechnung der Amtszeit als ruhegehaltsfähige Dienstzeit in entspre-chender Anwendung des Beamtenversorgungsgesetzes, wenn dies günstiger ist und der Bundesbeauftragte sich unmittel-bar vor seiner Wahl zum Bundesbeauf-tragten als Beamter oder Richter mindes-tens in dem letzten gewöhnlich vor Errei-chen der Besoldungsgruppe B 9 zu durch laufenden Amt befunden hat.	(7) [1]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. [2]Das Bundesreisekostengesetz und das Bundesumzugskostengesetz sind entsprechend anzuwenden. [3]Im übrigen sind die §§ 13 bis 20 des Bundesminister-gesetzes in der Fassung der Bekanntma-chung vom 27. Juli 1971 (BGBl. I S. 1166), zuletzt geändert durch das Gesetz zur Kür-zung des Amtsgehalts der Mitglieder der Bundesregierung und der Parlamentarischen Staatssekretäre vom 22. Dezember 1982 (BGBl. I S. 2007), mit der Maßgabe anzuwenden, dass an die Stelle der zweijährigen Amtszeit in § 15 Abs. 1 des Bundesministergesetzes eine Amtszeit von fünf Jahren tritt. [4]Abweichend von Satz 3 in Verbindung mit den §§ 15 bis 17 des Bundesministergesetzes berechnet sich das Ruhegehalt des Bundesbeauftragten unter Hinzurechnung der Amtszeit als ruhegehaltsfähige Dienstzeit in entsprechender Anwendung des Beamtenversorgungsgesetzes, wenn dies günstiger ist und der Bundesbeauftragte sich unmittel-bar vor seiner Wahl zum Bundesbeauf-tragten als Beamter oder Richter mindes-tens in dem letzten gewöhnlich vor Errei-chen der Besoldungsgruppe B 9 zu durch-laufenden 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	*Absatz 8 erweitert die Anwendung der Regelung des Absatzes 5 Satz 5 bis 7 auf die öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind.*

	den Datenschutz in den Ländern zuständig sind.	
§ 24 a.F.	§ 24 n.F.	
Kontrolle durch den Bundesbeauftragten für den Datenschutz	Kontrolle durch den Bundesbeauftragten für den Datenschutz	
(1) [1]Der Bundesbeauftragte für den Datenschutz kontrolliert bei den öffentlichen Stellen des Bundes die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz. [2]Werden personenbezogene Daten in Akten verarbeitet oder genutzt, kontrolliert der Bundesbeauftragte die Erhebung, Verarbeitung oder Nutzung, wenn der Betroffe-ne ihm hinreichende Anhaltspunkte dafür darlegt, daß er dabei in seinen Rechten verletzt worden ist, oder dem Bundesbe-auftragten hinreichende Anhaltspunkte für eine derartige Verletzung vorliegen.	(1) Der Bundesbeauftragte für den Datenschutz kontrolliert bei den öffentlichen Stellen des Bundes die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz.	*Die bisherige Beschränkung der Kontrolle des BfD in Akten auf eine Anlasskontrolle (Absatz 1 Satz 2) war zu streichen, da Artikel 28 der Richtlinie insoweit keine Einschränkung vorsieht. Unabhängig hiervon wird der BfD, sofern die kontrollierte Stelle den Sicherheitsvorbehalt nach § 24 Abs. 4 Satz 4 erhebt, zunächst die Entscheidung der obersten Bundesbehörde abwarten.*
(2) [1]Die Kontrolle des Bundesbeauftragten erstreckt sich auch auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis nach § 30 der Abgabenordnung, unterliegen. [2]Bei den Stellen des Bundes im Sinne des § 2 Abs. 1 Satz 2 wird das Postgeheimnis (Artikel 10 des Grundgesetzes) eingeschränkt, soweit dies zur Ausübung der Kontrolle bei den speichernden Stellen erforderlich ist. [3]Das Kontrollrecht erstreckt sich mit Ausnahme von Nummer 1 nicht auf den Inhalt des Post- und Fernmeldeverkehrs. [4]Der Kon-trolle durch den Bundesbeauftragten unter-liegen nicht: 1. personenbezogene Daten, die der Kontrolle durch die Kommission nach § 9 des Gesetzes zu Artikel 10 Grundge-	(2) [1]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. [2]Das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses des Artikels 10 des Grundgesetzes wird insoweit eingeschränkt. [3]Personenbezogene Daten, die der Kontrolle durch die Kommission nach § 9 des Gesetzes zu Artikel 10 Grundge-	*Bereits bei der Novellierung des BDSG 1990 waren zuvor bestehende Unsicherheiten in der Rechtsanwendungspraxis hinsichtlich personenbezogener Daten, die einem Be-rufs- oder besonderen Amtsgeheimnis unterliegen, durch Klarstellung im Rahmen der Neufassung von § 24 Abs. 1 und 2 beseitigt worden. Keine ausdrückliche Regelung enthält das geltende Recht für die Kontrolle des Bundesbeauftragten für den Daten-schutz hinsichtlich der von öffentlichen Stellen des Bundes erlangten personenbezoge-nen Daten über den Inhalt und die näheren Umstände des Brief-, Post- und Fernmelde-verkehrs. Vielmehr verwehrt § 24 Abs. 2 Satz 3 des geltenden Rechts, der den Inhalt des Post- und Fernmeldeverkehrs von der Kontrolle ausnimmt, es dem Bundesbeauf-tragten für den Datenschutz, die Verwendung der durch Eingriffe in das Brief-, Post- und Fernmeldegeheimnis erlangten Daten zu kontrollieren. Dies soll mit der vorgesehe-nen Änderung ermöglicht werden. Soweit der bisherige Satz 4 (zukünftig Satz 3) des § 24 Abs. 2 eine ausschließliche Kontrollkompetenz der in § 9 des Gesetzes zu Artikel 10 des Grundgesetzes genannten Kommission vorsieht, bleibt diese unberührt.* *Die Neuformulierung des Satzes 4 ist redaktionell bedingt durch die Streichung von Satz 4 Nr. 2 a.F.* *In Umsetzung von Artikel 28 der Richtlinie war in Absatz 2 Satz 4 a.F. das Widerspruchsrecht gegen die Kontrolle durch den Bundesbeauftragten für den Datenschutz,*

setz unterliegen, 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, und 2. a) personenbezogene Daten, die dem Post- und Fernmeldegeheimnis nach Artikel 10 des Grundgesetzes unterliegen, b) personenbezogene Daten, die dem Arztgeheimnis unterliegen und c) personenbezogene Daten in Personalakten oder in den Akten über die Sicherheitsüberprüfung, wenn der Betroffene der Kontrolle der auf ihn bezogenen Daten im Einzelfall gegen-über dem Bundesbeauftragten für den Datenschutz widerspricht. [5]Unbeschadet des Kontrollrechts des Bundesbeauftragten unterrichtet die öffentliche Stelle die Betroffenen in allgemeiner Form über das ihnen zustehende Widerspruchsrecht.	setz 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. [4]Der Kontrol-le 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.	*wie es in Absatz 2 Satz 4 Nr. 2 Buchstabe a und b sowie c 1. Teil (Personalakten) a.F. vorgesehen war, mit Blick auf die insoweit unbeschränkten Kontrollrechte nach Artikel 28 der Richtlinie zu streichen.*
(3) Die Bundesgerichte unterliegen der Kontrolle des Bundesbeauftragten nur, so-weit sie in Verwaltungsangelegenheiten tätig werden.	(3) Bei den Bundesgerichten ist die unmittelbar der Rechtsprechung dienende Tätigkeit der Richter von der Kontrolle ausgenommen.	*Die Neuregelung des Absatzes 3 präzisiert die Ausnahmen von der Kontrolle durch den Bundesbeauftragten für den Datenschutz im Bereich der Justiz.* ***Die Streichung*** [der vom RegE vorgesehenen Neuregelungen] ***führt zur Beibehaltung der bisherigen Gesetzesfassung, wonach die Kontrolle der Bundesgerichte durch den Bundesdatenschutzbeauftragten auf Verwaltungsangelegenheiten beschränkt ist. Die Streichung entspricht dem Vorschlag des Bundesrates (BR-Drs. 461/00 – Beschluss, S. 8, Nr. 9).***
(4) [1]Die öffentlichen Stellen des Bundes sind verpflichtet, den Bundesbeauftragten und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. [2]Ihnen ist dabei insbesondere 1. Auskunft zu ihren Fragen sowie Ein-	(4) [1]Die öffentlichen Stellen des Bundes sind verpflichtet, den Bundesbeauftragten und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. [2]Ihnen ist dabei insbesondere 1. Auskunft zu ihren Fragen sowie Ein-	

sicht in alle Unterlagen und Akten, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Kontrolle nach Absatz 1 stehen,	sicht 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.	2. jederzeit Zutritt in alle Diensträume zu gewähren.
[3]Die in § 6 Abs. 2 und § 19 Abs. 3 genannten Behörden gewähren die Unterstützung nur dem Bundesbeauftragten selbst und den von ihm schriftlich besonders Beauf-tragten. [4]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.	[3]Die in § 6 Abs. 2 und § 19 Abs. 3 genannten Behörden gewähren die Unterstützung nur dem Bundesbeauftragten selbst und den von ihm schriftlich besonders Beauf-tragten. [4]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) [1]Der Bundesbeauftragte teilt das Ergebnis seiner Kontrolle der öffentlichen Stelle mit. [2]Damit kann er Vorschläge zur Verbesserung des Datenschutzes, insbesondere zur Beseitigung von festgestellten Mängeln bei der Verarbeitung oder Nut-zung personenbezogener Daten, verbin-den. [3]§ 25 bleibt unberührt.	(5) [1]Der Bundesbeauftragte teilt das Ergebnis seiner Kontrolle der öffentlichen Stelle mit. [2]Damit kann er Vorschläge zur Verbesserung des Datenschutzes, insbesondere zur Beseitigung von festgestellten Mängeln bei der Verarbeitung oder Nut-zung personenbezogener Daten, verbin-den. [3]§ 25 bleibt unberührt.
(6) Absatz 2 gilt entsprechend für die öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind.	(6) Absatz 2 gilt entsprechend für die öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind.
§ 25 a.F.	§ 25 n.F.
Beanstandungen durch den Bundesbeauftragten für den Datenschutz	Beanstandungen durch den Bundesbeauftragten für den Datenschutz
(1) [1]Stellt der Bundesbeauftragte für den Datenschutz Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung	(1) [1]Stellt der Bundesbeauftragte für den Datenschutz Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung

oder Nutzung personenbezogener Daten fest, so beanstandet er dies

1. bei der Bundesverwaltung gegenüber der zuständigen obersten Bundesbe-hörde,
2. beim Bundeseisenbahnvermögen gegenüber dem Präsidenten,
3. bei den aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, so-lange ihnen ein ausschließliches Recht nach dem Postgesetz zusteht, gegen-über 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. [2]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 Män-gel handelt.

(3) [1]Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die auf Grund der Beanstandung des Bundesbeauftragten getroffen worden sind. [2]Die in Absatz 1 Satz 1 Nr. 4 genannten Stellen leiten der zuständigen Aufsichtsbehörde gleichzeitig eine Abschrift ihrer Stellung-

oder Nutzung personenbezogener Daten fest, so beanstandet er dies

1. bei der Bundesverwaltung gegenüber der zuständigen obersten Bundesbe-hörde,
2. beim Bundeseisenbahnvermögen gegenüber dem Präsidenten,
3. bei den aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, so-lange ihnen ein ausschließliches Recht nach dem Postgesetz zusteht, gegen-über 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. [2]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 Män-gel handelt.

(3) [1]Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die auf Grund der Beanstandung des Bundesbeauftragten getroffen worden sind. [2]Die in Absatz 1 Satz 1 Nr. 4 genannten Stellen leiten der zuständigen Aufsichtsbehörde gleichzeitig eine Abschrift ihrer Stellung-

nahme an den Bundesbeauftragten zu.	nahme an den Bundesbeauftragten zu.	
§ 26 a.F.	§ 26 n.F.	
Weitere Aufgaben des Bundesbeauftragten für den Datenschutz; Dateienregister	Weitere Aufgaben des Bundesbeauftragten für den Datenschutz	
(1) [1]Der Bundesbeauftragte für den Datenschutz erstattet dem Deutschen Bundestag alle zwei Jahre einen Tätigkeitsbericht. [2]Der Tätigkeitsbericht soll auch eine Dar-stellung der wesentlichen Entwicklung des Datenschutzes im nicht-öffentlichen Be-reich enthalten.	(1) [1]Der Bundesbeauftragte für den Datenschutz erstattet dem Deutschen Bundestag alle zwei Jahre einen Tätigkeitsbericht. [2]Er unterrichtet den Deutschen Bundestag und die Öffentlichkeit über wesentliche Entwicklungen des Datenschutzes.	*Absatz 1 Satz 2 beinhaltet eine ausdrückliche Befugnis des Bundesbeauftragten, sich jederzeit an Parlament und Öffentlichkeit wenden zu dürfen, um diese über wichtige Entwicklungen des Datenschutzes zu unterrichten.*
(2) [1]Auf Anforderung des Deutschen Bundestages oder der Bundesregierung hat der Bundesbeauftragte Gutachten zu er-stellen und Berichte zu erstatten. [2]Auf Er-suchen des Deutschen Bundestages, des Petitionsausschusses, des Innenausschus-ses oder der Bundesregierung geht der Bundesbeauftragte ferner Hinweisen auf Angelegenheiten und Vorgänge des Datenschutzes bei den öffentlichen Stellen des Bundes nach. [3]Der Bundesbeauftragte kann sich jederzeit an den Deutschen Bundestag wenden.	(2) [1]Auf Anforderung des Deutschen Bundestages oder der Bundesregierung hat der Bundesbeauftragte Gutachten zu er-stellen und Berichte zu erstatten. [2]Auf Er-suchen des Deutschen Bundestages, des Petitionsausschusses, des Innenausschus-ses oder der Bundesregierung geht der Bundesbeauftragte ferner Hinweisen auf Angelegenheiten und Vorgänge des Datenschutzes bei den öffentlichen Stellen des Bundes nach. [3]Der Bundesbeauftragte kann sich jederzeit an den Deutschen Bundestag wenden.	
(3) [1]Der Bundesbeauftragte kann der Bundesregierung und den in § 12 Abs. 1 genannten Stellen des Bundes Empfehlun-gen zur Verbesserung des Datenschutzes geben und sie in Fragen des Datenschut-zes beraten. [2]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.	(3) [1]Der Bundesbeauftragte kann der Bundesregierung und den in § 12 Abs. 1 genannten Stellen des Bundes Empfehlun-gen zur Verbesserung des Datenschutzes geben und sie in Fragen des Datenschut-zes beraten. [2]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 Stel-	(4) [1]Der Bundesbeauftragte wirkt auf die Zusammenarbeit mit den öffentlichen Stel-	*Absatz 4 Satz 2 erstreckt die Amtshilferegelung des § 38 Abs. 1 Satz 3 und 4 für die Aufsichtsbehörden auf den Bundesbeauftragten für den Datenschutz.*

len, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind, sowie mit den Aufsichtsbehörden nach § 38 hin.	len, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind, sowie mit den Aufsichtsbehörden nach § 38 hin. [2]§ 38 Abs. 1 Satz 3 und 4 gilt entsprechend.	*Nach § 4 d Abs. 1 und 2 in Verbindung mit § 4 f Abs. 1 Satz 1 entfällt aufgrund der obligatorischen Bestellung eines behördlichen Beauftragten für den Datenschutz die Meldepflicht im öffentlichen Bereich. Adressat der Verpflichtung nach § 4 g Abs. 2 ist im öffentlichen Bereich ausschließlich der Beauftragte für den Datenschutz. Die Notwendigkeit zur Führung eines Registers beim Bundesbeauftragten für den Datenschutz nach Absatz 5 a.F. entfällt daher.*
(5) [1]Der Bundesbeauftragte führt ein Register der automatisiert geführten Dateien, in denen personenbezogene Daten gespeichert werden. [2]Das gilt nicht für die Datei-en der in § 19 Abs. 3 genannten Behörden sowie für Dateien nach § 18 Abs. 3. [3]Die öffentlichen Stellen, deren Dateien in das Register aufgenommen werden, sind verpflichtet, dem Bundesbeauftragten eine Übersicht gemäß § 18 Abs. 2 Satz 2 Nr. 1 bis 6 zuzuleiten. [4]Das Register kann von jedermann eingesehen werden. [5]Die Angaben nach § 18 Abs. 2 Satz 2 Nr. 3 und 5 über Dateien der in § 6 Abs. 2 genannten Behörden unterliegen nicht der Einsichtnahme. [6]Der Bundesbeauftragte kann im Einzelfall für andere öffentliche Stellen mit deren Einverständnis festlegen, daß einzelne Angaben nicht der Einsichtnahme unterliegen.		
Dritter Abschnitt	**Dritter Abschnitt**	
Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen	**Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen**	
Erster Unterabschnitt	**Erster Unterabschnitt**	
Rechtsgrundlagen der Datenverarbeitung	**Rechtsgrundlagen der Datenverarbeitung**	

§ 27 a.F.	§ 27 n.F.	
Anwendungsbereich	Anwendungsbereich	
(1) [1]Die Vorschriften dieses Abschnittes finden Anwendung, soweit personenbezogene Daten in oder aus Dateien geschäftsmäßig oder für berufliche oder gewerbli-che Zwecke verarbeitet oder genutzt wer-den durch 1. nicht-öffentliche Stellen, 2. a) öffentliche Stellen des Bundes, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, b) öffentlichen Stellen der Länder, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, Bundesrecht ausführen und der Datenschutz nicht durch Landesgesetz geregelt ist. [2]In den Fällen der Nummer 2 Buchstabe a gelten anstelle des § 38 die §§ 18, 21 und 24 bis 26.	(1) [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) öffentlichen Stellen der Länder, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, Bundesrecht ausführen und der Datenschutz nicht durch Landesgesetz geregelt ist. [2]Dies gilt nicht, wenn die Erhebung, Verarbeitung oder Nutzung der Daten ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt. [3]In den Fällen der Nummer 2 Buchstabe a gelten anstelle des § 38 die §§ 18, 21 und 24 bis 26.	*Zu den Änderungen in Absatz 1 wird auf die Begründung zu § 1 Abs. 2 Nr. 3 sowie zu § 3 Abs. 2 verwiesen.* *Hinsichtlich der Einfügung des Wortes „erhoben“ in Absatz 1 wird auf die Begründung zu § 4 Abs. 1 verwiesen*
(2) Die Vorschriften dieses Abschnittes gelten nicht für die Verarbeitung und Nutzung personenbezogener Daten in Akten, soweit es sich nicht um personenbezogene Daten handelt, die offensichtlich aus einer Datei entnommen worden sind.	(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.	*Die Änderung in Absatz 2 ist eine Folgeänderung im Zusammenhang mit der Änderung des Dateibegriffs und der Tatsache, dass dem Begriff der Akte keine eigenständige Bedeutung mehr zukommt (vgl. hierzu die Begründung zu § 3 Abs. 2).*

§ 28 a.F.	§ 28 n.F.	
Datenspeicherung, -übermittlung und -nutzung für eigene Zwecke	Datenerhebung, -verarbeitung und -nut-zung für eigene Zwecke	
(1) [1]Das Speichern, Verändern oder Über-	(1) [1]Das Erheben, Speichern, Verändern	*Absatz 1 Satz 1 bedurfte der Ergänzung durch den Begriff der Erhebung, da Artikel 2*
mitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung ei-gener Geschäftszwecke ist zulässig	oder Übermitteln personenbezogener Da-ten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig	*Buchstabe b der Richtlinie die Erhebung als Verarbeitungsform begreift, und die in Artikel 7 aufgeführten Voraussetzungen für die Zulässigkeit der Verarbeitung damit auch bei der Erhebung personenbezogener Daten zu beachten sind. Absatz 1 Satz 2 a.F. konnte daher entfallen.*
1. im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen,	1. wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient,	*Die Neuformulierung von Absatz 1 Nr. 1 verdeutlicht den Gedanken der Zweckbestimmung. Die Änderungen in Absatz 1 Nr. 2 und 3 sowie in Absatz 4 („verantwortliche Stelle“) sind Folgeänderungen im Zusammenhang mit der Ersetzung des Begriffs der speichernden Stelle durch den der verantwortlichen Stelle (vgl. hierzu die Begründung zu § 3 Abs. 7). Die übrigen Änderungen in Absatz 1 Nr. 3 verdeutlichen, dass eine Ab-wägung der schutzwürdigen Interessen des Betroffenen mit dem berechtigten Interesse der verantwortlichen Stelle stattfinden muss.*
2. soweit es zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und kein Grund zu der Annahme besteht, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Verarbeitung oder Nutzung überwiegt,	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 Nut-zung überwiegt oder	*Absatz 1 Nr. 4 a.F. beinhaltete - insofern atypisch im Vergleich zu Absatz 1 Nr. 1 bis 3 - eine Zweckänderungsregelung, die fast wörtlich der Zweckänderungsregelung in § 14 Abs. 2 Nr. 9 entsprach. In Übereinstimmung mit der Systematik des Absatzes 1 Nr. 1 bis 3 und um Überschneidungen mit Absatz 3 Nr. 4 zu vermeiden, war Absatz 1 Nr. 4 aufzuheben. Die Zulässigkeit des Erhebens im Bereich der wissenschaftlichen Forschung bleibt hiervon unberührt und richtet sich wie bisher nach Absatz 1 Nr. 1 und 2.*
3. wenn die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die speichernde Stelle sie veröffentlichen dürfte, es sei denn, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Verarbeitung oder Nutzung offensichtlich überwiegt,	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.	*Artikel 6 Abs. 1 Buchstabe b der Richtlinie sieht vor, dass personenbezogene Daten „für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit die-sen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden“. Gemäß Artikel 10 der Richtlinie ist der Betroffene bereits bei der Erhebung über die Zweckbestimmungen der Erhebung, Verarbeitung und Nutzung zu informieren. Dies setzt voraus, dass bereits bei der Erhebung der Zweck festliegen muss.*
4. wenn es im Interesse der speichernden Stelle zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorha-bens das Interesse des Betroffenen an dem Ausschluß der Zweckänderung erheblich überwiegt und der Zweck der	[2]Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen.	[Neufassung des § 28 Abs. 1 Satz 1 Nr. 3 ist] ***Folgeänderung zu*** [§ 10 Abs. 5] ***(Vereinheitlichung des Sprachgebrauchs durch Ersetzung der Worte „aus allgemein zugänglichen Quellen“ durch die Worte „allgemein zugänglich“).***

Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. [2]Die Daten müssen nach Treu und Glau-ben und auf rechtmäßige Weise erhoben werden.		
	(2) Für einen anderen Zweck dürfen sie nur unter den Voraussetzungen des Absatzes 1 Satz 1 Nr. 2 und 3 übermittelt oder genutzt werden.	*Da die Richtlinie nicht zwischen dem öffentlichen und dem nicht-öffentlichen Bereich differenziert, Artikel 6 Absatz 1 Buchstabe b der Richtlinie somit auch im nicht-öffentlichen Bereich uneingeschränkt Anwendung findet, war der Grundsatz der Zweckbin-dung daher hier weitergehend als bisher zu verankern. Absatz 2 beinhaltet deswegen eine entsprechende über Absatz 4 a.F. hinausgehende Zweckänderungsregelung. Da Fälle einer Zweckänderung unter den Voraussetzungen des Absatzes 1 Nr. 1 nicht vor-stellbar sind, konnte der Verweis auf Absatz 1 Nr. 2 und 3 beschränkt werden.*
(2) [1]Die Übermittlung oder Nutzung ist auch zulässig 1. a) soweit es zur Wahrung berechtigter Interessen eines Dritten oder öffentlicher Interessen erforderlich ist oder b) wenn es sich um listenmäßig oder sonst zusammengefaßte Daten über Angehörige einer Personengruppe handelt, die sich auf - eine Angabe über die Zugehörigkeit des Betroffenen zu dieser Personengruppe, - Berufs-, Branchen- oder Geschäftsbezeichnung, - Namen, - Titel, - akademische Grade, - Anschrift, - Geburtsjahr beschränken und kein Grund zu der Annahme besteht, daß der Betroffe-	(3) Die Übermittlung oder Nutzung für ei-nen 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 Geschäftsbeziehung, c) Namen, d) Titel, e) akademische Grade, f) Anschrift und	*Die Neufassung von Absatz 3 beruht im wesentlichen auf rechtsförmlichen Überlegungen. Absatz 3 Satz 1 Nr. 2 entspricht Absatz 2 Nr. 1 a, zweite Alternative a.F. In Übereinstimmung mit Artikel 6 und 13 der Richtlinie war der Begriff des öffentlichen Interesses auf den der Abwehr von Gefahren für die staatliche und öffentliche Sicherheit so-wie der Verfolgung von Straftaten zu begrenzen. Durch die Änderung in Absatz 3 Satz 1 Nr. 3 wird die Zweckbindung in Umsetzung von Artikel 6 Abs. 1 Buchstabe b der Richtlinie verankert und gleichzeitig der betroffene Adressatenkreis der Regelung ver-deutlicht. Da der Betroffene in den Fällen des Absatzes 3 Nrn. 1 bis 3 nicht nur ein schutzwürdiges Interesse am Ausschluss der Übermittlung, sondern auch der Nutzung haben kann, war Absatz 3 Satz 1 a.F. entsprechend zu ergänzen. Die Streichung des Merkmals „gesundheitliche Verhältnisse“ in Absatz 3 Satz 2 beruht auf der Einfügung des Absatzes 6, der für die besonderen Arten personenbezogener Daten (§ 3 Abs. 9), und damit auch für Gesundheitsdaten, eine enge Verwendungsbeschränkung vorsieht.*

ne ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat. [2]In den Fällen des Buchstabens b kann im allgemeinen davon ausgegangen werden, daß dieses Interesse besteht, wenn im Rahmen der Zweckbestim-mung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhält-nisses gespeicherte Daten übermittelt werden sollen, die sich auf - auf gesundheitliche Verhältnisse, - auf strafbare Handlungen, - auf Ordnungswidrigkeiten, - auf religiöse oder politische Anschauungen sowie - bei Übermittlung durch den Arbeitgeber auf arbeitsrechtliche Rechtsverhältnisse beziehen, oder 2. 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 Wei-se nicht oder nur mit unverhältnismä-ßigem Aufwand erreicht werden kann.	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 un-verhältnismäßigem 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.	
(3) [1]Widerspricht der Betroffene bei der speichernden 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. [2]Wider-	(4) [1]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. [2] Der	*Satz 2 setzt Artikel 14 Satz 2 der Richtlinie um, wonach die Mitgliedstaaten die erforderlichen Maßnahmen zu ergreifen haben, um sicherzustellen, dass die betroffenen Personen vom Bestehen des Widerspruchsrechts Kenntnis haben. Damit der Adressat des Widerspruchsrechts insbesondere im Rahmen von schriftlichen Werbeaktionen ermittelt werden kann, ist eine Information über die verantwortliche Stelle vorgesehen.* ***Die Änderung*** [des Abs. 4 Satz 2] ***folgt dem Vorschlag des Bundesrates (BR-***

spricht der Betroffene beim Empfänger der nach Absatz 2 übermittelten Daten der Verarbeitung oder Nutzung zum Zwecke der Werbung oder der Markt- oder Meinungsforschung, hat dieser die Daten für diese Zwecke zu sperren.	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 Da-ten 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. [3]Widerspricht der Betroffenen bei dem Drittten, dem die Da-ten 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.	***Drs. 461/00 – Beschluss, S. 9, Nr. 11) unter Berücksichtigung der in der Gegenäußerung der Bundesregierung (BT-Drs. 14/4458, S. 2, Nr. 11) vorgeschlagenen Änderung.*** ***Der Bundesrat hat seinen Vorschlag wie folgt begründet: „Mit der Ergänzung soll klargestellt werden, dass die Verpflichtung, dem Betroffenen die Kenntnis über die Quelle seiner für die Werbung genutzten Daten zu verschaffen, auch dann besteht, wenn der Werbetreibende fremde Datenbestände insbesondere im sog. Listbroking-verfahren einsetzen lässt. ... Damit der Betroffene das Widerspruchsrecht effektiv wahrnehmen kann, muss er jedoch die Möglichkeit haben, sich auf einfache Weise Kenntnis über die Quelle seiner Daten zu verschaffen. Dazu reicht die Verpflichtung aus, dem Betroffenen bei der werblichen Ansprache eine Nachfragemöglichkeit nach dem Adresslisteneigner zu eröffnen, der seine Daten für die Werbung zur Verfügung gestellt hat. Dies kann beispielsweise durch die Angabe einer Telefonnummer im Werbemittel realisiert werden, die zu einer Stelle geschaltet ist, welche über die Zuordnung der Daten zum Adresseigner informieren und ggf. Widersprüche des Betroffenen entgegennehmen kann.“*** ***Die Ergänzung des § 28 Abs. 4 führt im Ergebnis zu einer Verbesserung der Rechtsstellung des Betroffenen. Die Pflicht sicherzustellen, „dass der Betroffene Kenntnis über die Herkunft der Daten erhalten kann“, kann auf verschiedene Weise erfüllt werden. Neben dem vom Bundesrat genannten Beispiel ist auch eine Lösung denkbar und z.B. für einen Werbeadressaten auch einfacher, nach der die Unterrichtung durch den Ansprechenden selbst erfolgt, etwa indem dieser den Datenmakler vertraglich verpflichtet, ihm – zur Weiterleitung an den Betroffenen – im Einzelfall die Herkunft der entsprechenden Daten offen zu legen.*** *Da es sich bei der Regelung des Absatzes 4 Satz 3 um ein Widerspruchsrecht des Betroffenen gegenüber demjenigen handelt, an den Daten des Betroffenen übermittelt wurden, also gegenüber einem Dritten, war der weitergehende Begriff des Empfängers durch den des Dritten zu ersetzen*
(4) [1]Der Empfänger darf die übermittelten Daten für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. [2]Eine Verarbeitung oder Nutzung für andere Zwecke ist nur unter den Voraussetzungen der Absätze 1 und 2 zulässig. [3]Die übermittelnde Stelle hat den Empfänger darauf hinzuweisen.	(5) [1]Der Dritte, dem die Daten übermittelt worden sind, darf diese nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. [2]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. [3]Die übermittelnde Stelle hat ihn darauf hinzuweisen.	*Im Hinblick auf Absatz 5 Satz 1 wird auf die Begründung zu Absatz 4 Satz 3 verwiesen. Die Änderungen in Absatz 5 Satz 2 beseitigen eine redaktionelle Unschärfe der bisherigen Regelung.*

(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.

Absätze 6 bis 9 setzen Artikel 8 der Richtlinie um. Auf dem Gebiet des Arbeitsrechts können für die Verwendung der in § 3 Abs. 9 genannten Arten personenbezogener Da-ten bereichsspezifische Regelungen geschaffen werden. Das ist durch Artikel 8 Abs. 2 Buchstabe b der Richtlinie gedeckt. Die in § 3 Abs. 9 genannten Daten dürfen im übrigen auch bisher nur im Rahmen der Grundsätze des allgemeinen arbeitsrechtlichen Informations- und Datenschutzes erhoben, verarbeitet und genutzt werden, die die von der Richtlinie vorgesehenen Garantien enthalten.

Nummer 1 des Absatzes 6 setzt Artikel 8 Abs. 2 Buchstabe c der Richtlinie um.

Nummern 2 und 3 des Absatzes 6 setzen Artikel 8 Abs. 2 Buchstabe e der Richtlinie um. Die nach Nummer 3 vorzunehmende Abwägung trägt dem Umstand Rechnung, dass die Berücksichtigung der Belange des Betroffenen nach Absatz 1 Nr. 2 bereits für Daten gilt, die nicht § 3 Abs. 9 unterfallen.

Zu Absatz 6 Nummer 4 wird auf die Ausführungen zu § 13 Abs. 2 Nr. 8 verwiesen.

(7) [1]Das Erheben von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) ist ferner zulässig, wenn dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von

Zu Absatz 7 wird auf die Begründung zu § 13 Abs. 2 Nr. 7 verwiesen. Satz 3 ist eine Auffangnorm für Leistungserbringer, die zu Lasten der Sozialversicherungssysteme abrechnen.

Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheim-haltungspflicht unterliegen. [2]Die Verarbei-tung und Nutzung von Daten zu den in Satz 1 genannten Zwecken rich-tet sich nach den für die in Satz 1 genann-ten Personen gel-tenden Geheimhaltungspflichten. [3]Werden zu einem in Satz 1 ge-nannten Zweck Da-ten über die Gesundheit von Personen durch Angehörige eines an-deren als in § 203 Abs. 1 und 3 des Strafgesetzbuches genannten Berufes, dessen Ausübung die Feststellung, Heilung oder Linderung von Krankheiten oder die Herstellung oder den Vertrieb von Hilfsmitteln mit sich bringt, erhoben, verarbeitet oder genutzt, ist dies nur unter den Voraussetzungen zulässig, unter denen ein Arzt selbst hierzu befugt wäre.	
(8) [1]Für einen anderen Zweck dürfen die besonderen Arten personenbezogener Da-ten (§ 3 Abs. 9) nur unter den Voraussetzungen des Absatzes 6 Nr. 1 bis 4 oder des Absatzes 7 Satz 1 übermittelt oder ge-nutzt werden. [2]Eine Übermittlung oder Nutzung ist auch zulässig, wenn dies zur Abwehr von erheblichen Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfol-gung von Straftaten von erheblicher Bedeu-tung erforderlich ist.	*Absatz 8 Satz 1 entspricht der Regelung des Absatzes 2 und verankert auch hier den Grundsatz der Zweckbindung nach Artikel 6 Abs. 1 Buchstabe b der Richtlinie. Satz 2 regelt einen zusätzlichen Fall zulässiger Zweckänderung, der mit Artikel 8 Abs. 4 der Richtlinie in Einklang steht.*
(9) [1]Organisationen, die politisch, philoso-phisch, religiös oder gewerkschaftlich aus-gerichtet sind und keinen Erwerbszweck verfolgen, dürfen besondere Arten perso-nenbezogener Daten (§ 3 Abs. 9) erheben, verarbeiten oder nutzen, soweit dies für die Tätigkeit der Organisation erforderlich ist. [2]Dies gilt nur für personenbezogene Daten	*Absatz 9 setzt Artikel 8 Abs. 2 Buchstabe d der Richtlinie um.*

	ihrer Mitglieder oder von Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßig Kontakte mit ihr unterhalten. [3]Die Übermittlung dieser personenbezogenen Daten an Personen oder Stellen außerhalb der Organisation ist nur unter den Voraussetzungen des § 4a Abs. 3 zulässig. [4]Absatz 3 Nr. 2 gilt entsprechend.	
§ 29 a.F.	§ 29 n.F.	
Geschäftsmäßige Datenspeicherung zum Zwecke der Übermittlung	Geschäftsmäßige Datenerhebung und -speicherung zum Zwecke der Übermittlung	
(1) [1]Das geschäftsmäßige Speichern oder Verändern personenbezogener Daten zum Zwecke der Übermittlung ist zulässig, wenn 1. kein Grund zu der Annahme besteht, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Speicherung oder Veränderung hat, oder 2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die speichernde Stelle sie veröffentlichen dürfte, es sei denn, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Speicherung oder Veränderung offensichtlich überwiegt. [2]§ 28 Abs. 1 Satz 2 ist anzuwenden.	(1) [1]Das geschäftsmäßige Erheben, Speichern oder Verändern personenbezogener Daten zum Zwecke der Übermittlung, insbesondere wenn dies der Werbung, der Tätigkeit von Auskunfteien, dem Adresshandel oder der Markt- und Meinungsforschung dient, ist zulässig, wenn 1. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung oder Veränderung hat, oder 2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Speicherung oder Veränderung offensichtlich überwiegt. [2]§ 28 Abs. 1 Satz 2 ist anzuwenden.	*Hinsichtlich der Einfügung des Begriffs der Erhebung in die Überschrift sowie in Absatz 1 wird auf die Begründung zu § 28 Abs. 1 verwiesen.* *Der nunmehr verwandte Begriff der verantwortlichen Stelle ist in der Begründung zu § 3 Abs. 7 erläutert* *Die Ergänzungen von Absatz 1 vor Nummer 1 verstärken den Grundsatz der Zweckbindung im Rahmen der Vorschrift. Auf die Begründung zu § 28 Abs. 2 wird insoweit verwiesen.*
(2) [1]Die Übermittlung ist zulässig, wenn 1. a) der Empfänger ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat oder	(2) [1]Die Übermittlung im Rahmen der Zwecke nach Absatz 1 ist zulässig, wenn 1. a) der Dritte, dem die Daten übermit-telt werden, ein berechtigtes Interes-se	*Der Einschub in Absatz 2 vor Nummer 1 a stellt sicher, dass Übermittlungen gemäß Absatz 2 nur bei Vorliegen der Zwecke des Absatzes 1 vorgenommen werden dürfen.* *Die Vorschrift erfasst nicht-öffentliche Stellen, die geschäftsmäßig Daten speichern, um sie zu übermitteln, also an Dritte bekanntzugeben (§ 3 Abs. 4 Satz 2 Nr. 3). Um Miss-*

b) es sich um listenmäßig oder sonst zusammengefaßte Daten nach § 28 Abs. 2 Nr. 1 Buchstabe behandelt, die für Zwecke der Werbung oder der Markt- oder Meinungsforschung übermittelt werden sollen, und 2. kein Grund zu der Annahme besteht, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat. [2]§ 28 Abs. 2 Nr. 1 Satz 2 gilt entsprechend. [3]Bei der Übermittlung nach Nummer 1 Buchstabe a sind die Gründe für das Vorliegen eines berechtigten Interesses und die Art und Weise ihrer glaubhaften Darlegung von der übermittelnden Stelle aufzuzeichnen. [4]Bei der Übermittlung im automatisierten Abrufverfahren obliegt die Aufzeichnungspflicht dem Empfänger.	an ihrer Kenntnis glaubhaft dargelegt hat oder b) es sich um listenmäßig oder sonst zusammengefasste Daten nach § 28 Abs. 3 Nr. 3 handelt, die für Zwecke der Werbung oder der Markt- oder Meinungsforschung übermittelt werden sollen, und 2. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. [2]§ 28 Abs. 3 gilt entsprechend. [3]Bei der Übermittlung nach Nummer 1 Buchsta-be a sind die Gründe für das Vorliegen eines berechtigten Interesses und die Art und Weise ihrer glaubhaften Darlegung von der übermittelnden Stelle aufzuzeich-nen. [4]Bei der Übermittlung im automati-sierten Abrufverfahren obliegt die Aufzeichnungspflicht dem Dritten, dem die Daten übermittelt werden.	*verständnisse mit dem weitergehenden Begriff des nun in § 3 Abs. 8 Satz 1 definierten Empfängers zu vermeiden, war der Begriff des Empfängers durch den des Dritten, dem die Daten übermittelt werden, zu ersetzen.* *Die Änderungen der Verweise in Absatz 2 Satz 1 Nr. 1 b sowie Satz 2 sind Folgeänderungen im Zusammenhang mit der Einfügung eines neuen Absatzes 2 in § 28 und der Neugestaltung des Absatzes 3.*
(3) Für die Verarbeitung oder Nutzung der übermittelten Daten gilt § 28 Abs. 3 und 4.	(3) Die Aufnahme personenbezogener Daten in elektronische oder gedruckte Adress-, Telefon-, Branchen- oder vergleichbare Verzeichnisse hat zu unterbleiben, wenn der entgegenstehende Wille des Betroffenen aus dem zugrunde liegen-den 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.	*§ 10 Telekommunikationsdiensteunternehmen-Datenschutzverordnung (TDSV) erlaubt, dass sog. Diensteanbieter, d.h. alle, die ganz oder teilweise geschäftsmäßig Telekommunikationsleistungen erbringen, Verzeichnisse ihrer Kunden als Druckwerke oder elektronisch herstellen und diese selbst oder durch Dritte herausgeben. Hierin werden die Kunden auf freiwilliger Basis mit ihrem Namen und ihrer Anschrift eingetragen. Der Kunde hat die Möglichkeit, seiner Eintragung in elektronischen und gedruckten Ver-zeichnissen jeweils gesondert zu widersprechen. Der Widerspruch muss in den Kundenverzeichnissen kenntlich gemacht werden. Da die Vorschrift des § 10 TDSV als Normadressaten nur Diensteanbieter erfasst, besteht eine Regelungslücke für denjenigen Personenkreis, der – ohne Diensteanbieter zu sein – vergleichbare Verzeichnisse erstellt. Auch Adressbücher werden zunehmend in elektronischer Form erstellt. Bislang galten insoweit nur die allgemeinen Vorschriften des Bundesdatenschutzgesetzes, die sich als unzureichend erwiesen haben.* *Der neue Absatz 3 schafft nun Rechtsklarheit insofern, als er sicherstellt, dass der Wille von Betroffenen, nicht eingetragen zu werden, von jedem potenziellen Herausgeber entsprechender Verzeichnisse dahingehend zu respektieren ist, dass die Aufnahme in Adress- u.ä. Verzeichnisse zu unterbleiben hat oder bei der Übernahme in Verzeichnis-*

		se oder Register entsprechende Markierungen übernommen werden müssen. Voraussetzung hierfür ist die Kenntlichmachung des einer Eintragung entgegenstehenden Willens in dem Verzeichnis oder Register, das von dem potentiellen Herausgeber als Grundlage für sein eigenes Verzeichnis herangezogen wird. Dies ist bereichsspezifisch zu regeln.
	(4) Für die Verarbeitung oder Nutzung der übermittelten Daten gilt § 28 Abs. 4 und 5.	*Die geänderten Verweise in Absatz 4 sind Folgeänderungen im Zusammenhang mit der Schaffung eines neuen Absatzes 2 in § 28.*
	(5) § 28 Abs. 6 bis 9 gilt entsprechend.	*Absatz 5 stellt sicher, dass die Restriktionen für die Erhebung, Verarbeitung und Nutzung sensitiver Daten auch im Anwendungsbereich von § 29 gelten.*
§ 30 a.F.	§ 30 n.F.	
Geschäftsmäßige Datenspeicherung zum Zwecke der Übermittlung in anonymisierter Form	Geschäftsmäßige Datenerhebung und -speicherung zum Zwecke der Übermittlung in anonymisierter Form	
(1) [1]Werden personenbezogene Daten geschäftsmäßig 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. [2]Diese Merkmale dürfen mit den Einzelangaben nur zusammengeführt werden, soweit dies für die Erfüllung des Zweckes der Speiche-rung oder zu wissenschaftlichen Zwecken erforderlich ist.	(1) [1]Werden personenbezogene Daten geschäftsmäßig erhoben und gespeichert, um sie in anonymisierter Form zu übermit-teln, sind die Merkmale gesondert zu spei-chern, mit denen Einzelangaben über per-sönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürli-chen Person zugeordnet werden können. [2]Diese Merkmale dürfen mit den Einzelan-gaben nur zusammengeführt werden, so-weit dies für die Erfüllung des Zweckes der Speicherung oder zu wissenschaftlichen Zwecken erforderlich ist.	*Hinsichtlich der Einfügung des Begriffs der Erhebung in die Überschrift sowie in Absatz 1 wird auf die Begründung zu § 28 Abs. 1 verwiesen.*
(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 speichernde Stelle sie veröffentlichen dürfte, es sei denn, daß das	(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	*Bezüglich des Begriffs der verantwortlichen Stelle in Absatz 2 Nr. 2 wird auf die Begründung zu § 3 Abs. 7 verwiesen.Die Formulierung „soweit nicht“ in Absatz 2 Nr. 2 verdeutlicht das Erfordernis einer Abwägung mit den schutzwürdigen Interessen des Betroffenen.*

schutzwürdige Interesse des Betroffenen an dem Ausschluß der Veränderung offensichtlich überwiegt.	schutzwürdige Interesse des Betroffenen an dem Ausschluss der Veränderung offensichtlich überwiegt.	
(3) Die personenbezogenen Daten sind zu löschen, wenn ihre Speicherung unzuläs-sig ist.	(3) Die personenbezogenen Daten sind zu löschen, wenn ihre Speicherung unzuläs-sig ist.	
(4) Die §§ 29, 33 bis 35 gelten nicht.	(4) § 29 gilt nicht.	*Da die Vereinbarkeit des Ausschlusses der Betroffenenrechte in Absatz 4 mit Artikel 13 der Richtlinie zweifelhaft ist, war die Verweisung in Absatz 4 insoweit zu streichen.*
	(5) § 28 Abs. 6 bis 9 gilt entsprechend.	*Auf die Begründung zu § 29 Abs. 5 wird verwiesen.*
§ 31 a.F.	§ 31 n.F.	
Besondere Zweckbindung	Besondere Zweckbindung	
Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstel-lung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespei-chert werden, dürfen nur für diese Zwecke verwendet werden.	Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstel-lung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespei-chert werden, dürfen nur für diese Zwecke verwendet werden.	
§ 32 a.F.	§ 32 n.F.	
Meldepflichten	Meldepflichten	
(1) Die Stellen, die personenbezogene Daten geschäftsmäßig 1. zum Zwecke der Übermittlung speichern, 2. zum Zwecke der anonymisierten Übermittlung speichern oder 3. im Auftrag als Dienstleistungsunternehmen verarbeiten oder nutzen, sowie ihre Zweigniederlassungen und unselbständigen Zweigstellen haben die Aufnahme und Beendigung ihrer Tätigkeit der zuständigen Aufsichtsbehörde innerhalb eines Monats mitzuteilen.	weggefallen	*Die Aufhebung von § 32 a.F. ist eine Folgeänderung im Zusammenhang mit den neu geschaffenen Vorschriften der §§ 4 d und 4 e.*

(2) Bei der Anmeldung sind folgende Angaben für das bei der Aufsichtsbehörde geführte Register mitzuteilen:

1. Name oder Firma der Stelle,
2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzlich oder nach der Verfassung des Unternehmens berufe-ne Leiter und die mit der Leitung der Datenverarbeitung beauftragten Perso-nen,
3. Anschrift,
4. Geschäftszwecke der Stelle und der Datenverarbeitung,
5. Name des Beauftragten für den Datenschutz,
6. allgemeine Beschreibung der Art der gespeicherten personenbezogenen Daten. Im Falle des Absatzes 1 Nr. 3 ist diese Angabe nicht erforderlich.

(3) Bei der Anmeldung sind außerdem folgende Angaben mitzuteilen, die nicht in das Register aufgenommen werden:

1. Art der eingesetzten Datenverarbei-tungsanlagen,
2. bei regelmäßiger Übermittlung personenbezogener Daten Empfänger und Art der übermittelten Daten.

(4) Absatz 1 gilt für die Änderung der nach Absätzen 2 und 3 mitgeteilten Angaben entsprechend.

(5) [1]Die Aufsichtsbehörde kann im Einzelfall festlegen, welche Angaben nach Absatz 2 Nr. 4 und 6, Absatz 3 und Absatz 4 mitgeteilt werden müssen. [2]Der mit den Mitteilungen verbundene Aufwand muß in einem angemessenen Verhältnis zu ihrer

Bedeutung für die Überwachung durch die Aufsichtsbehörde stehen.		
Zweiter Unterabschnitt **Rechte des Betroffenen**	**Zweiter Unterabschnitt** **Rechte des Betroffenen**	
§ 33 a.F.	§ 33 n.F.	
Benachrichtigung des Betroffenen	Benachrichtigung des Betroffenen	
(1) [1]Werden erstmals personenbezogene Daten für eigene Zwecke gespeichert, ist der Betroffene von der Speicherung und der Art der Daten zu benachrichtigen. [2]Werden personenbezogene Daten ge-schäftsmäßig zum Zwecke der Übermitt-lung gespeichert, ist der Betroffene von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichti-gen.	(1) [1]Werden erstmals personenbezogene Daten für eigene Zwecke ohne Kenntnis des Betroffenen gespeichert, ist der Be-troffene von der Speicherung, der Art der Daten, der Zweckbestimmung der Erhe-bung, Verarbeitung oder Nutzung und der Identität der verantwortlichen Stelle zu be-nachrichtigen. [2]Werden personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen. [3]Der Betroffene ist in den Fällen der Sätze 1 und 2 auch über die Kategorien von Empfängern zu unterrichten, soweit er nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss.	*Durch die Erweiterung der Benachrichtigungspflicht gegenüber dem Betroffenen in Absatz 1 Satz 1 und 3 wird Artikel 11 Abs. 1 der Richtlinie für den nicht-öffentlichen Bereich umgesetzt.*
(2) Eine Pflicht zur Benachrichtigung besteht nicht, wenn	(2) [1]Eine Pflicht zur Benachrichtigung besteht nicht, wenn	
1. der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat,	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 Datenschutz-	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 Datenschutz-	*Die bisher geltende Ausnahme von der Benachrichtigung in Absatz 2 Nr. 2 war auf-grund des in Artikel 11 Abs.2 der Richtlinie vorgesehenen Gedankens des Absehens von der Benachrichtigung aus Gründen der Unverhältnismäßigkeit entsprechend einzu-schränken.*

kontrolle dienen,	kontrolle 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, geheimgehal-ten werden müssen,	3. die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheimgehal-ten werden müssen,	
4. die zuständige öffentliche Stelle gegenüber der speichernden Stelle festge-stellt hat, daß das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,	4. die Speicherung oder Übermittlung durch Gesetz ausdrücklich vorgesehen ist,	*Durch die neu eingefügte Nummer 4 wird der Ausnahmekatalog des Absatzes 2 um einen in Artikel 11 Abs. 2 der Richtlinie vorgesehenen Ausnahmetatbestand ergänzt.* *Anwendungsbeispiel ist etwa das Geldwäschegesetz vom 25. Oktober 1993, (BGBl. I S. 1770, zuletzt geändert durch Gesetz vom 17. Dezember 1997, BGBl. I S. 3108). Hier entfällt eine Benachrichtigungspflicht aufgrund der im Geldwäschegesetz ausdrücklich vorgesehenen Speicherungs- und Übermittlungsvorschriften der hiervon betroffenen Institute.*
5. die Daten in einer Datei gespeichert werden, die nur vorübergehend vorgehalten und innerhalb von drei Monaten nach ihrer Erstellung gelöscht wird,	5. die Speicherung oder Übermittlung für Zwecke der wissenschaftlichen Forschung erforderlich ist und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde,	*Hinsichtlich der Aufhebung von Absatz 2 Nr. 5 a.F. wird auf die Begründung zur Aufhebung von § 18 Abs. 3 verwiesen* *Die neu eingefügte Nummer 5 setzt Artikel 11 Abs. 2 der Richtlinie um, soweit dort eine Ausnahme von der Benachrichtigungspflicht im Rahmen der Datenverarbeitung für Zwecke der wissenschaftlichen Forschung vorgesehen ist.*
6. die Daten für eigene Zwecke gespeichert sind und a) aus allgemein zugänglichen Quellen entnommen sind oder b) die Benachrichtigung die Geschäftszwecke der speichernden Stelle erheblich gefährden würde, es sei denn, daß das Interesse an der Benachrichtigung die Gefährdung überwiegt, oder	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 geschäftsmäßig zum Zwecke der Übermittlung gespeichert sind und a) aus allgemein zugänglichen Quellen entnommen sind, soweit sie sich auf diejenigen Personen beziehen, die diese Daten veröffentlicht haben,	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 unverhältnismä-ßig ist,	*Auf die Begründung zu Absatz 2 Nr. 2 wird verwiesen.*

oder	oder	
b) es sich um listenmäßig oder sonst zusammengefaßte Daten handelt (§ 29 Abs. 2 Nr. 1 Buchstabe b).	b) die Benachrichtigung die Geschäftszwecke der verantwortlichen Stelle erheblich gefährden würde, es sei denn, dass das Interesse an der Benachrichtigung die Gefährdung überwiegt, oder	
	8. die Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert sind und a) aus allgemein zugänglichen Quellen entnommen sind, soweit sie sich auf diejenigen Personen beziehen, die diese Daten veröffentlicht haben, oder b) es sich um listenmäßig oder sonst zusammengefasste Daten handelt (§ 29 Abs. 2 Nr. 1 Buchstabe b) und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist.	*Auf die Begründung zu Absatz 2 Nr. 2 wird verwiesen.*
	[2]Die verantwortliche Stelle legt schriftlich fest, unter welchen Voraussetzungen von einer Benachrichtigung nach Satz 1 Nr. 2 bis 7 abgesehen wird.	*Durch Absatz 2 Satz 2 wird das Erfordernis der „geeigneten Garantien“ gemäß Arti-kel 11 Abs. 2 Satz 2 der Richtlinie umgesetzt. Der betriebliche Beauftragte für den Datenschutz wirkt auf die Einhaltung dieser Vorschrift hin.*
§ 34 a.F.	§ 34 n.F.	
Auskunft an den Betroffenen	Auskunft an den Betroffenen	
(1) [1]Der Betroffene kann Auskunft verlangen über	(1) [1]Der Betroffene kann Auskunft verlangen über	*Durch die Neufassung wird Artikel 12 Buchstabe a, 1. Spiegelstrich der Richtlinie umgesetzt.*
1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf Herkunft und Empfänger beziehen,	1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,	*Die Neufassung erweitert den Umfang des Auskunftsrechts um die Information über Empfänger oder Kategorien von Empfängern. Um inhaltliche Überschneidungen von Nummer 2 mit Nummer 1 a.F. zu vermeiden, war Nummer 1 entsprechend zu modifizieren. Im Hinblick auf den Begriff des Empfängers wird auf § 3 Abs. 8 Satz 1 sowie die Begründung hierzu verwiesen. Das Kriterium der Regelmäßigkeit (vgl. Nummer 3 a.F.) war zu streichen, da die Richtlinie keine entsprechende Einschränkung vorsieht. Die Änderung des Satzes 3 beruht auf einer Anpassung an die Ausnahme vom Auskunfts-recht*
2. den Zweck der Speicherung und	2. Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben werden, und	
3. Personen und Stellen, an die seine Daten regelmäßig übermittelt werden, wenn		

seine Daten automatisiert verar-beitet werden.	3. den Zweck der Speicherung.	*nach Artikel 13 Buchstabe g der Richtlinie. Der Schutz der „Rechte und Freiheiten anderer Personen“ umfasst auch das Geschäftsgeheimnis.*
[2]Er soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnen. [3]Werden die personenbezogenen Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert, kann der Betroffene über Herkunft und Empfänger nur Auskunft verlangen, wenn er begründete Zweifel an der Richtigkeit der Daten geltend macht. [4]In diesem Falle ist Auskunft über Herkunft und Empfänger auch dann zu erteilen, wenn diese Anga-ben nicht gespeichert sind.	[2]Er soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnen. [3]Werden die personenbezogenen Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert, kann der Betroffene über Herkunft und Empfänger nur Auskunft verlangen, so-fern nicht das Interesse an der Wahrung des Geschäftsgeheimnisses überwiegt. [4]In diesem Falle ist Auskunft über Herkunft und Empfänger auch dann zu erteilen, wenn diese Angaben nicht gespeichert sind.	
(2) [1]Der Betroffene kann von Stellen, die geschäftsmäßig personenbezogene Daten zum Zwecke der Auskunftserteilung speichern, Auskunft über seine personenbezogenen Daten verlangen, auch wenn sie nicht in einer Datei gespeichert sind. [2]Aus-kunft über Herkunft und Empfänger kann der Betroffene nur verlangen, wenn er be-gründete Zweifel an der Richtigkeit der Da-ten geltend macht. [3]§ 38 Abs. 1 ist mit der Maßgabe anzuwenden, daß die Aufsichts-behörde im Einzelfall die Einhaltung von Satz 1 überprüft, wenn der Betroffene be-gründet darlegt, daß die Auskunft nicht oder nicht richtig erteilt worden ist.	(2) [1]Der Betroffene kann von Stellen, die geschäftsmäßig personenbezogene Daten zum Zwecke der Auskunftserteilung speichern, Auskunft über seine personenbezogenen Daten verlangen, auch wenn sie weder in einer automatisierten Verarbeitung noch in einer nicht automatisierten Datei gespeichert sind. [2]Auskunft über Herkunft und Empfänger kann der Betroffene nur verlangen, sofern nicht das Interesse an der Wahrung des Geschäftsgeheimnisses überwiegt.	*Absatz 2 Satz 3 a.F. war in Übereinstimmung mit Artikel 28 der Richtlinie aufzuheben. Zu Satz 2 wird auf die Begründung zu Absatz 1 verwiesen.*
(3) Die Auskunft wird schriftlich erteilt, soweit nicht wegen der besonderen Umstände eine andere Form der Auskunftserteilung angemessen ist.	(3) Die Auskunft wird schriftlich erteilt, soweit nicht wegen der besonderen Umstände eine andere Form der Auskunftserteilung angemessen ist.	
(4) Eine Pflicht zur Auskunftserteilung besteht nicht, wenn der Betroffene nach § 33 Abs. 2 Nr. 2 bis 6 nicht zu benachrichtigen ist.	(4) Eine Pflicht zur Auskunftserteilung besteht nicht, wenn der Betroffene nach § 33 Abs. 2 Satz 1 Nr. 2, 3 und 5 bis 7 nicht zu benachrichtigen ist.	*Anders als im Rahmen der Benachrichtigung sind im Rahmen der Auskunft Ausnah-men in den Fällen des § 33 Abs. 2 Nr. 2, 4 und 5 nicht sachgerecht. Die Verweisung in § 33 Abs. 4 war dementsprechend zu begrenzen.* ***Die Anpassung*** [Verweis auch auf § 33 Abs. 2 Nr. 2, 5 und 7] ***setzt eine Prüfbitte des Bundesrates um (vgl. BR-Drs. 461/00 – Beschluss, S. 4, Nr. 2, 6. Anstrich). Sie stellt***

		die nach der Richtlinie zulässigen Ausnahmetatbestände der bisherigen Gesetzesfassung – eingeschränkt – wieder her.
		Durch die Änderung wird gegenüber der Fassung des Regierungsentwurfs das Auskunftsrecht nur in Ausnahmefällen begrenzt. Die in § 33 Abs. 2 Nrn. 2, 5 und 7 Buchstabe a zugunsten von Betroffenen eingeführte Änderung, derzufolge von einer Benachrichtigung nur abgesehen werden darf, wenn sie einen unverhältnismäßigen Aufwand erfordert, bleibt auch im Rahmen des geänderten § 34 erhalten.
		Der vom Bundesrat ebenfalls vorgeschlagenen Begrenzung der Auskunftspflicht nach § 6a Abs. 3 im Interesse des Schutzes der Betriebs- und Geschäftsgeheimnisse der verantwortlichen Stelle trägt der Regierungsentwurf bereits Rechnung, da sich die Auskunftspflicht nur auf den logischen Aufbau der automatisierten Verarbeitung, nicht aber beispielsweise auf Auskünfte über die verwendete Software bezieht.
		Zu § 6a ist jedoch noch folgende Klarstellung geboten: Entgegen der Begründung des Regierungsentwurfs kommt es bei § 6a für die Beurteilung, ob eine Entscheidung ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt wird, nicht darauf an, ob das Scoring-Verfahren und die abschließende Entscheidung in einer Hand liegen. Der Schutzgedanke des § 6a geht vielmehr davon aus, dass – soweit nach Absatz 2 die berechtigten Interessen des Betroffenen berührt sind und nicht anderweitig gewahrt werden –, eine Bewertung von Persönlichkeitsmerkmalen, wie z. B. der Kreditwürdigkeit, in jedem Fall eine Beurteilung durch einen Menschen erfordert, die das Ergebnis einer standardisierten Computeranalyse nicht zur einzigen Entscheidungsgrundlage macht, sondern Raum lässt für eine Überprüfung und Relativierung dieses Ergebnisses, insbesondere auf Grund eigener zusätzlicher Erkenntnisse oder besonderer Umstände des Einzelfalls.
(5) [1]Die Auskunft ist unentgeltlich. [2]Werden die personenbezogenen Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert, kann jedoch ein Entgelt verlangt werden, wenn der Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen kann. [3]Das Entgelt darf über die durch die Auskunftserteilung entstandenen direkt zurechenbaren Kosten nicht hinausgehen. [4]Ein Entgelt kann in den Fällen nicht verlangt werden, in denen besondere Umstände die Annahme rechtfertigen, daß Daten unrichtig oder unzulässig gespeichert werden, oder in denen die	(5) [1]Die Auskunft ist unentgeltlich. [2]Werden die personenbezogenen Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert, kann jedoch ein Entgelt verlangt werden, wenn der Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen kann. [3]Das Entgelt darf über die durch die Auskunftserteilung entstandenen direkt zurechenbaren Kosten nicht hinausgehen. [4]Ein Entgelt kann in den Fällen nicht verlangt werden, in denen besondere Umstände die Annahme rechtfertigen, dass Daten unrichtig oder unzulässig gespeichert werden, oder in denen	

Auskunft ergibt, daß die Daten zu berichtigen oder unter der Voraussetzung des § 35 Abs. 2 Satz 2 Nr. 1 zu löschen sind.	die Auskunft ergibt, dass die Daten zu berichtigen oder unter der Voraussetzung des § 35 Abs. 2 Satz 2 Nr. 1 zu löschen sind.	
(6) [1]Ist die Auskunftserteilung nicht unentgeltlich, ist dem Betroffenen die Möglichkeit zu geben, sich im Rahmen seines Auskunftsanspruchs persönlich Kenntnis über die ihn betreffenden Daten und Angaben zu verschaffen. [2]Er ist hierauf in geeigneter Weise hinzuweisen.	(6) [1]Ist die Auskunftserteilung nicht unentgeltlich, ist dem Betroffenen die Möglichkeit zu geben, sich im Rahmen seines Auskunftsanspruchs persönlich Kenntnis über die ihn betreffenden Daten und Angaben zu verschaffen. [2]Er ist hierauf in geeigneter Weise hinzuweisen.	
§ 35 a.F.	§ 35 n.F.	
Berichtigung, Löschung und Sperrung von Daten	Berichtigung, Löschung und Sperrung von Daten	
(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind.	(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind.	
(2) [1]Personenbezogene Daten können außer in den Fällen des Absatzes 3 Nr. 1 und 2 jederzeit gelöscht werden. [2]Personenbezogene Daten sind zu löschen, wenn	(2) [1]Personenbezogene Daten können außer in den Fällen des Absatzes 3 Nr. 1 und 2 jederzeit gelöscht werden. [2]Personenbezogene Daten sind zu löschen, wenn	
1. ihre Speicherung unzulässig ist,	1. ihre Speicherung unzulässig ist,	
2. es sich um Daten über gesundheitliche Verhältnisse, strafbare Handlungen, Ordnungswidrigkeiten sowie religiöse oder politische Anschauungen handelt und ihre Richtigkeit von der speichernden Stelle nicht bewiesen werden kann,	2. es sich um Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit, über Gesundheit oder das Sexualleben, strafbare Handlungen oder Ordnungswidrigkeiten handelt und ihre Richtigkeit von der verantwortlichen Stelle nicht bewiesen werden kann,	*Absatz 2 Satz 2 Nr. 2 ist um die Merkmale von Artikel 8 der Richtlinie ergänzt. Im Hinblick auf die Ersetzung der Wörter „speichernde Stelle“ durch die Wörter „verantwortli-che Stelle“ wird auf die Begründung zu § 3 Abs. 7 verwiesen.*
3. sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zweckes der Speicherung nicht mehr erforderlich ist, oder	3. sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zweckes der Speicherung nicht mehr erforderlich ist, oder	
4. sie geschäftsmäßig zum Zwecke der Übermittlung verarbeitet werden und eine	4. sie geschäftsmäßig zum Zweck der Übermittlung verarbeitet werden und eine	*Durch die Änderungen in Absatz 2 Satz 2 Nr. 4 wird sichergestellt, dass bei Daten, die geschäftsmäßig zum Zwecke der Übermittlung verarbeitet werden, jeweils nach vier Jah-*

Prüfung am Ende des fünften Kalenderjahres nach ihrer erstmaligen Speicherung ergibt, daß eine längerwährende Speicherung nicht erforder-lich ist.	Prüfung jeweils am Ende des vier-ten Kalenderjahres beginnend mit ihrer erstmaligen Speicherung ergibt, dass eine längerwährende Speicherung nicht erforderlich ist.	*ren eine Überprüfung ihrer Erforderlichkeit erfolgt.*
(3) An die Stelle einer Löschung tritt eine Sperrung, soweit	(3) An die Stelle einer Löschung tritt eine Sperrung, soweit	
1. im Falle des Absatzes 2 Nr. 3 oder 4 einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,	1. im Falle des Absatzes 2 Nr. 3 einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,	
2. Grund zu der Annahme besteht, daß durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder	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.	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.	(4) Personenbezogene Daten sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.	
(5) [1]Personenbezogene Daten, die unrichtig sind oder deren Richtigkeit bestritten wird, müssen bei der geschäftsmäßigen Datenspeicherung zum Zwecke der Übermittlung außer in den Fällen des Absatzes 2 Nr. 2 nicht berichtigt, gesperrt oder gelöscht werden, wenn sie aus allgemein zugänglichen Quellen entnommen und zu Dokumentationszwecken gespeichert sind. [2]Auf Verlangen des Betroffenen ist diesen Daten für die Dauer der Speicherung seine Gegendarstellung beizufügen. [3]Die Daten dürfen nicht ohne diese Gegendarstellung übermittelt werden.	(5) [1]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. [2]Satz 1 gilt nicht, wenn eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung verpflichtet.	

(6) 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 regelmäßigen Datenübermittlung diese Da-ten zur Speicherung weitergegeben wer-den, wenn dies zur Wahrung der schutzwürdigen Interessen des Betroffenen erforderlich ist.	(6) [1]Personenbezogene Daten, die unrichtig sind oder deren Richtigkeit bestritten wird, müssen bei der geschäftsmäßigen Datenspeicherung zum Zwecke der Übermittlung außer in den Fällen des Absatzes 2 Nr. 2 nicht berichtigt, gesperrt oder gelöscht werden, wenn sie aus allgemein zugänglichen Quellen entnommen und zu Dokumentationszwecken gespeichert sind. [2]Auf Verlangen des Betroffenen ist diesen Daten für die Dauer der Speicherung seine Gegendarstellung beizufügen. [3]Die Daten dürfen nicht ohne diese Gegendarstellung übermittelt werden.	
(7) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn 1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweis-not oder aus sonstigen im überwiegen-den Interesse der speichernden Stelle oder eines Dritten liegenden Gründen unerläßlich ist und 2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.	(7) Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu verständigen, denen im Rahmen einer Datenübermittlung diese Daten zur Speicherung weitergegeben werden, wenn dies keinen unverhältnismäßigen Aufwand erfordert und schutzwürdige Interessen des Betroffenen nicht entgegenstehen.	*Durch den Wegfall der Regelmäßigkeit der Datenübermittlung in Absatz 7 als Voraussetzung der Nachberichtspflicht (vgl. Absatz 6 a.F.) wird in Umsetzung von Artikel 12 Buchstabe c der Richtlinie der Anwendungsbereich der Nachberichtspflicht erweitert. Gleichzeitig wird - ebenfalls in Umsetzung der Richtlinie - sichergestellt, dass die Nachberichtspflicht nur besteht, wenn sie keinen unverhältnismäßigen Aufwand erfordert.* *Durch die Formulierung „und schutzwürdige Interessen des Betroffenen nicht entgegenstehen“ soll verhindert werden, dass eine Benachrichtigung zu Lasten des Betroffenen erfolgen kann.*
	(8) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn 1 es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweis-not oder aus sonstigen im überwiegen-den Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerlässlich ist und 2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht ge-	*Die Änderung in Absatz 8 Nr. 1 ist eine Folgeänderung im Zusammenhang mit der Ersetzung des Begriffs der speichernden Stelle durch den der verantwortlichen Stelle (vgl. hierzu die Begründung zu § 3 Abs. 7).*

	sperrt wären.	
Dritter Unterabschnitt **Beauftragter für den Datenschutz, Aufsichtsbehörde**	**Dritter Unterabschnitt** **Aufsichtsbehörde**	
§ 36 a.F.	§ 36 n.F.	
Bestellung eines Beauftragten für den Datenschutz	Bestellung eines Beauftragten für den Datenschutz	
(1) [1]Die nicht-öffentlichen Stellen, die personenbezogene Daten automatisiert verarbeiten und damit in der Regel mindestens fünf Arbeitnehmer ständig beschäftigen, haben spätestens innerhalb eines Monats nach Aufnahme ihrer Tätigkeit einen Beauftragten für den Datenschutz schriftlich zu bestellen. [2]Das gleiche gilt, wenn personenbezogene Daten auf andere Weise verarbeitet werden und damit in der Regel mindestens zwanzig Arbeitnehmer ständig beschäftigt sind.	weggefallen	*Die Regelungen über den betrieblichen Beauftragten für den Datenschutz wurden im Dritten Abschnitt aufgehoben und finden sich nunmehr in den §§ 4 f und 4 g. Die Überschrift des Dritten Unterabschnitts war daher anzupassen.* *Die Aufhebung von § 36 ist eine Folgeänderung im Zusammenhang mit der neu geschaffenen Vorschrift des § 4 f.*
(2) Zum Beauftragten für den Datenschutz darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt.		
(3) [1]Der Beauftragte für den Datenschutz ist dem Inhaber, dem Vorstand, dem Geschäftsführer oder dem sonstigen gesetzlich oder nach der Verfassung des Unternehmens berufenen Leiter unmittelbar zu unterstellen. [2]Er ist bei Anwendung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. [3]Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. [4]Die Bestellung zum Beauftragten für den Datenschutz kann nur auf Verlangen der Aufsichtsbehörde oder in		

entsprechender Anwendung von § 626 des Bürgerlichen Gesetzbuchs widerrufen werden.		
(4) Der Beauftragte für den Datenschutz ist zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit er nicht davon durch den Betroffenen befreit wird.		
(5) Die nicht-öffentliche Stelle hat den Beauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen und ihm insbesondere, soweit dies zur Er-füllung seiner Aufgaben erforderlich ist, Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stel-len.		
§ 37 a.F.	§ 37 n.F.	
Aufgaben des Beauftragten für den Datenschutz	Aufgaben des Beauftragten für den Datenschutz	
(1) [1]Der Beauftragte für den Datenschutz hat die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz sicherzustellen. [2]Zu diesem Zweck kann er sich in Zweifelsfällen an die Aufsichtsbehörde wenden. [3]Er hat insbesondere	weggefallen	*Die Aufhebung von § 37 ist eine Folgeänderung im Zusammenhang mit der neu geschaffenen Vorschrift des § 4 g.*
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 ande-		

ren Vorschriften über den Datenschutz, bezogen auf die besonderen Verhältnisse in diesem Geschäftsbereich und die sich daraus ergebenden besonde-ren Erfordernisse für den Datenschutz, vertraut zu machen, 3. bei der Auswahl der bei der Verarbeitung personenbezogener Daten tätigen Personen beratend mitzuwirken. (2) Dem Beauftragten ist von der nicht-öffentlichen Stelle eine Übersicht zur Verfügung zu stellen über 1. eingesetzte Datenverarbeitungsanla-gen, 2. Bezeichnung und Art der Dateien, 3. Art der gespeicherten Daten, 4. Geschäftszwecke, zu deren Erfüllung die Kenntnis dieser Daten erforderlich ist, 5. deren regelmäßige Empfänger, 6. zugriffsberechtigte Personengruppen oder Personen, die allein zugriffsberechtigt sind. (3) Absatz 2 Nr. 2 bis 6 gilt nicht für Dateien, die nur vorübergehend vorgehalten und innerhalb von drei Monaten nach ihrer Erstellung gelöscht werden.		
§ 38 a.F. Aufsichtsbehörde (1) Die Aufsichtsbehörde überprüft im Einzelfall die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die Verarbeitung oder Nutzung personenbezogener Daten in oder aus Dateien regeln, wenn ihr hinreichende Anhaltspunkte dafür vorliegen, daß eine	§ 38 n.F. Aufsichtsbehörde (1) [1]Die Aufsichtsbehörde kontrolliert die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz, so-weit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten	*Artikel 28 der Richtlinie sieht keine Beschränkung der Datenschutzkontrolle auf eine Anlasskontrolle vor, wie sie in Absatz 1 a.F. geregelt war. Die entsprechenden Einschränkungen in Absatz 1 a.F. waren daher zu streichen, das Wort „überprüft“ durch das Wort „kontrolliert“ zur Vereinheitlichung der Terminologie zu ersetzen. Zu den Vorschriften, deren Ausführung die Aufsichtsbehörde kontrolliert, zählen auch die Verhaltensregeln nach § 38 a.* *Die Ergänzung „einschließlich ... § 1 Abs. 5“ in Absatz 1 Satz 1 stellt in Übereinstim-*

dieser Vorschriften durch nicht-öffentliche Stellen verletzt ist, insbesondere wenn es der Betroffene selbst begründet darlegt.	Dateien regeln einschließlich des Rechts der Mitgliedstaaten in den Fällen des § 1 Abs. 5. [2]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. [3]Insbesondere darf die Aufsichtsbehörde zum Zweck der Aufsicht Daten an andere Aufsichtsbehörden übermitteln. [4]Sie leistet den Aufsichtsbehörden anderer Mitgliedstaaten der Europäischen Union auf Ersuchen ergänzende Hilfe (Amtshilfe). [5]Stellt die Aufsichtsbehörde einen Ver-stoß 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. [6]Sie veröffentlicht regelmäßig, spätestens alle zwei Jahre, einen Tätigkeitsbericht. [7]§ 21 Satz 1 und § 23 Abs. 5 Satz 4 bis 7 gelten entsprechend.	*mung mit Artikel 28 Abs. 6 Satz 1 der Richtlinie sicher, dass die Aufsichtsbehörde auch in den Fällen, in denen nach § 1 Abs. 5 Recht anderer Mitgliedstaaten zur Anwendung gelangt, zuständig ist.* *Absatz 1 Sätze 2, 3 und 5 legt auf der einen Seite die Zweckbindung der von der Aufsichtsbehörde gespeicherten Daten fest und regelt näher die notwendigen Datenübermittlungen der Aufsichtsbehörde an andere Stellen.* *Durch Absatz 1 Satz 4 wird in Umsetzung von Artikel 28 Abs. 6 Satz 1 und 2 der Richtlinie die Amtshilfe unter den Aufsichtsbehörden der Mitgliedstaaten der Europäischen Union geregelt* *Durch Absatz 1 Satz 6 wird Artikel 28 Abs. 5 der Richtlinie umgesetzt. Die gewählte Frist entspricht der Verpflichtung des Bundesbeauftragten für den Datenschutz nach § 26 Abs. 1 Satz 1, alle zwei Jahre einen Tätigkeitsbericht vorzulegen.* *Absatz 1 Satz 7 gewährleistet entsprechend Artikel 28 Abs. 4 Satz 1 der Richtlinie Betroffenen ein Anrufungsrecht gegenüber der Aufsichtsbehörde und stellt sicher, dass die in § 23 Abs. 5 benannten Vorschriften der Abgabenordnung nicht gelten. Ferner beinhaltet Satz 7 eine Anzeigebefugnis der Aufsichtsbehörde sowie deren Recht, Betroffene hierüber zu informieren. Auf die Begründung zu § 23 Abs. 5 wird verwiesen. Artikel 28 Abs. 2 der Richtlinie war nicht umzusetzen, da die Länder bei der Ausarbeitung von Vorschriften im Sinne des Artikels 28 Abs. 2 der Richtlinie ohnehin angehört werden und diese wiederum gemäß Absatz 6 die Aufsichtsbehörden bestimmen.* *Der Bundesbeauftragte für den Datenschutz ist gemäß § 26 Abs. 3 bereits gegenwärtig an der Erarbeitung von Rechtsvorschriften zu beteiligen. Da für die Mitarbeiter der Aufsichtsbehörden und des Bundesbeauftragten für den Datenschutz ähnliche Vorschriften über die Verschwiegenheitspflicht gelten (vgl. insoweit für Beamte § 39 BRRG, §§ 61, 62 BBG, für Angestellte § 9 BAT und Arbeiter § 11 MTArb), war Artikel 28 Abs. 7 der Richtlinie für die Mitarbeiter dieser Behörden nicht umzusetzen.*
(2) [1]Werden personenbezogene Daten geschäftsmäßig 1. zum Zwecke der Übermittlung gespeichert, 2. zum Zwecke der anonymisierten Übermittlung gespeichert oder 3. im Auftrag durch Dienstleistungsunternehmen verarbeitet, überwacht die Aufsichtsbehörde die Ausführung dieses Gesetzes oder anderer Vor-	(2) [1]Die Aufsichtsbehörde führt ein Register der nach § 4d meldepflichtigen automatisierten Verarbeitungen mit den Angaben nach § 4e Satz 1. [2]Das Register kann von jedem eingesehen werden. [3]Das Einsichtsrecht erstreckt sich nicht auf die Angaben nach § 4e Satz 1 Nr. 9 sowie auf die Angabe der zugriffsberechtigten Personen.	*Absatz 2 Satz 1a.F. konnte aufgehoben werden, da aufgrund des Wegfalls der Beschränkung auf die Anlasskontrolle in Absatz 1 der Grund für die unterschiedlichen Reelnigen in Absatz 1 und 2 weggefallen ist. Die Änderung von Satz 2 ist eine Folgeänderung im Zusammenhang mit der Aufhebung des § 32 Abs. 2 und der neu geschaffenen Vorschrift des § 4 d. Satz 2 entspricht Absatz 2 Satz 3 a.F. Satz 3 entspricht der Regelung des § 4 g Abs. 2 Satz 2.*

schriften über den Datenschutz, soweit diese die Verarbeitung oder Nutzung personenbezogener Daten in oder aus Datei-en regeln. [2]Die Aufsichtsbehörde führt das Register nach § 32 Abs. 2. [3]Das Register kann von jedem eingesehen werden.		
(3) [1]Die der Prüfung unterliegenden Stel-len sowie die mit deren Leitung beauftrag-ten Personen haben der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unver-züglich zu erteilen. [2]Der Auskunftspflich-tige 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 An-gehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. [3]Der Auskunftspflichtige ist darauf hinzuweisen.	(3) [1]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. [2]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. [3]Der Auskunftspflichtige ist darauf hinzuweisen.	***Die Änderungen*** [der Abs. 3, 4 und 6 : jeweils Ersetzung der Wörter „Prüfung“, „Überprüfung“ und „Überwachung“ durch das Wort „Kontrolle“] ***folgen Vorschlägen des Bundesrates (BR-Drs. 461/00 – Beschluss, S. 12, Nr. 13), der für § 38 zur Herstellung eines einheitlichen Sprachgebrauchs die durchgehende Verwendung des Wortes „Kontrolle“ angeregt hat.***
(4) [1]Die von der Aufsichtsbehörde mit der Überprüfung oder Überwachung 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. [2]Sie können geschäftliche Unterlagen, insbesondere die Übersicht nach § 37 Abs. 2 sowie die gespeicherten personenbezogenen Daten und die Datenverarbeitungsprogramme, einsehen. § 24 Abs. 6 gilt entsprechend. [3]Der Auskunftspflichtige hat diese Maß-nahmen zu dulden.	(4) [1]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. [2]Sie können geschäftliche Unterlagen, insbesondere die Übersicht nach § 4g Abs. 2 Satz 1 sowie die gespeicherten personenbezogenen Daten und die Datenverarbeitungsprogramme, einsehen. [3]§ 24 Abs. 6 gilt entsprechend. [4]Der Auskunftspflichtige hat diese Maßnahmen zu dulden.	*Die Änderung des Verweises in Absatz 4 Satz 2 ist eine Folgeänderung im Zusammenhang mit der Aufhebung der Vorschrift des § 37 Abs. 2 a.F.*
(5) [1]Zur Gewährleistung des Datenschutzes nach diesem Gesetz und anderen Vor-	(5) [1]Zur Gewährleistung des Datenschutzes nach diesem Gesetz und anderen Vor-	*Im Hinblick auf die Einfügung des Wortes „Erhebung“ wird auf die Begründung zu § 28 Abs. 1, im Hinblick auf die Einfügung der Worte „automatisierte Verarbeitung personen-*

schriften über den Datenschutz, soweit diese die Verarbeitung oder Nutzung personenbezogener Daten in oder aus Datei-en regeln, kann die Aufsichtsbehörde anordnen, daß im Rahmen der Anforderun-gen nach § 9 Maßnahmen zur Beseitigung festgestellter technischer oder organisatorischer Mängel getroffen werden. 2Bei schwerwiegenden Mängeln dieser Art, insbesondere, wenn sie mit besonderer Gefährdung des Persönlichkeitsrechts verbunden sind, kann sie den Einsatz einzelner Verfahren untersagen, wenn die Män-gel entgegen der Anordnung nach Satz 1 und trotz der Verhängung eines Zwangs-geldes nicht in angemessener Zeit besei-tigt werden. 3Sie kann die Abberufung des Beauftragten für den Datenschutz verlan-gen, wenn er die zur Erfüllung seiner Auf-gaben erforderliche Fachkunde und Zuver-lässigkeit nicht besitzt.	schriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln, kann die Aufsichtsbehörde anordnen, dass im Rahmen der Anforderungen nach § 9 Maßnahmen zur Beseitigung festgestellter technischer oder organisatorischer Mängel getroffen werden. 2Bei schwerwiegenden Mängeln dieser Art, insbesondere, wenn sie mit besonderer Gefährdung des Persönlichkeitsrechts verbunden sind, kann sie den Einsatz einzelner Verfahren untersagen, wenn die Mängel entgegen der An-ordnung nach Satz 1 und trotz der Verhän-gung eines Zwangsgeldes nicht in angemessener Zeit beseitigt werden. 3Sie kann die Abberufung des Beauftragten für den Datenschutz verlangen, wenn er die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit nicht besitzt.	*bezogener Daten oder die Verarbeitung personenbezogener Daten in oder aus nicht-automatisierten Dateien“ auf die Begründung zu § 3 Abs. 2 verwiesen.*
(6) Die Landesregierungen oder die von ihnen ermächtigten Stellen bestimmen die für die Überwachung der Durchführung des Datenschutzes im Anwendungsbereich dieses Abschnittes zuständigen Aufsichts-behörden.	(6) Die Landesregierungen oder die von ihnen ermächtigten Stellen bestimmen die für die Kontrolle der Durchführung des Datenschutzes im Anwendungsbereich dieses Abschnittes zuständigen Aufsichtsbehör-den.	
(7) Die Anwendung der Gewerbeordnung auf die den Vorschriften dieses Abschnitts unterliegenden Gewerbebetriebe bleibt un-berührt.	(7) Die Anwendung der Gewerbeordnung auf die den Vorschriften dieses Abschnitts unterliegenden Gewerbebetriebe bleibt unberührt.	
	§ 38 a n.F.	
	Verhaltensregeln zur Förderung der Durchführung datenschutzrechtlicher Regelungen	
	(1) Berufsverbände und andere Vereinigungen, die bestimmte Gruppen von verantwortlichen Stellen vertreten, können Entwürfe für	*Diese Vorschrift setzt Artikel 27 der Richtlinie um. Die Verhaltensregeln des Absatzes 1 sollen als interne Regelungen zur ordnungsgemäßen Durchführung datenschutzrechtlicher Regelungen beitragen. Berufsverbände und die anderen in Absatz 1 genannten*

	Verhaltensregeln zur Förderung der Durchführung von datenschutzrechtlichen Regelungen der zuständigen Aufsichtsbehörde unterbreiten.	*Vereinigungen erhalten die Möglichkeit, von ihnen erarbeitete Verhaltensregeln der Aufsichtsbehörde zur Überprüfung vorzulegen. Die Entwürfe sind in rechtlicher, techni-scher und organisatorischer Hinsicht ausreichend zu begründen und auf Verlangen der Aufsichtsbehörde zu erläutern.*
	(2) Die Aufsichtsbehörde überprüft die Vereinbarkeit der ihr unterbreiteten Ent-würfe mit dem geltenden Datenschutz-recht.	*Die Verpflichtung der Aufsichtsbehörde zur Überprüfung ihr vorgelegter Entwürfe an-hand des geltenden Datenschutzrechts gemäß Absatz 2 soll verhindern, dass Berufs-verbände und die anderen in Absatz 1 genannten Vereinigungen sich interne Verhal-tensregeln geben, die im Widerspruch zu den gesetzlichen Regelungen stehen.*
Vierter Abschnitt **Sondervorschriften**	**Vierter Abschnitt** **Sondervorschriften**	
§ 39 a.F.	§ 39 n.F.	
Zweckbindung bei personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen	Zweckbindung bei personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen	
(1) [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 speichernden Stelle nur für den Zweck verarbeitet oder genutzt werden, für den sie sie erhalten hat. [2]In die Übermittlung an eine nicht-öffentliche Stelle muß die zur Verschwiegenheit verpflichtete Stelle einwilligen.	(1) [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. [2]In die Übermittlung an eine nicht-öffentliche Stelle muss die zur Verschwiegenheit verpflichtete Stelle einwilligen.	*Die Änderung in Absatz 1 Satz 1 ist eine Folgeänderung im Zusammenhang mit der Ersetzung des Begriffs der speichernden Stelle durch den der verantwortlichen Stelle (vgl. hierzu die Begründung zu § 3 Abs. 7).*
(2) Für einen anderen Zweck dürfen die Daten nur verarbeitet oder genutzt werden, wenn die Änderung des Zwecks durch besonderes Gesetz zugelassen ist.	(2) Für einen anderen Zweck dürfen die Daten nur verarbeitet oder genutzt werden, wenn die Änderung des Zwecks durch besonderes Gesetz zugelassen ist.	
§ 40 a.F.	§ 40 n.F.	
Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen	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.	(1) Für Zwecke der wissenschaftlichen Forschung erhobene oder gespeicherte personenbezogene Daten dürfen nur für Zwecke der wissenschaftlichen Forschung verarbeitet oder genutzt werden.	*Im Gegensatz zu Absatz 1, der sowohl für öffentliche als auch für nicht-öffentliche Stellen gilt, enthielt Absatz 2 a.F. eine Sonderregelung für die Übermittlung an „andere als öffentliche Stellen". Inhaltlich beschränkte sich Absatz 2 a. F. auf die Verpflichtung zur Abgabe einer Erklärung zur Einhaltung des Gebotes der Zweckbindung und der Beachtung des Absatzes 3 durch die Stelle, an die übermittelt wird. Da die Stelle, an die die Daten nach Absatz 2 a.F. übermittelt werden, aber ohnehin unter die Regelung des § 40 fällt, die Verpflichtungen gemäß den Absätzen 1 und 3 a.F. somit gelten, konnte Absatz 2 aufgehoben werden.*
(2) Die Übermittlung personenbezogener Daten an andere als öffentliche Stellen für Zwecke der wissenschaftlichen Forschung ist nur zulässig, wenn diese sich verpflichten, die übermittelten Daten nicht für andere Zwecke zu verarbeiten oder zu nutzen und die Vorschrift des Absatzes 3 einzuhalten.	(2) [1]Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist. [2]Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer be-stimmten oder bestimmbaren Person zu-geordnet werden können. [3]Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert.	
(3) [1]Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist. [2]Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer be-stimmten oder bestimmbaren Person zu-geordnet werden können. [3]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.	
(4) 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 a.F.	§ 41 n.F.	

Verarbeitung und Nutzung personenbezogener Daten durch die Medien	Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die Medien	
(1) [1]Soweit personenbezogene Daten von Unternehmen oder Hilfsunternehmen der Presse oder des Films oder von Hilfsunternehmen des Rundfunks ausschließlich zu eigenen journalistisch-redaktionellen Zwecken verarbeitet oder genutzt werden, gelten von den Vorschriften dieses Gesetzes nur die §§ 5 und 9. [2]Soweit Verlage personenbezogene Daten zur Herausgabe von Adressen-, Telefon-, Branchen- oder vergleichbaren Verzeichnissen verarbeiten oder nutzen, gilt Satz 1 nur, wenn mit der Herausgabe zugleich eine journalistisch-redaktionelle Tätigkeit verbunden ist.	(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.	*Anstelle der bisher in Absatz 1 enthaltenen Vollregelung beinhaltet Absatz 1 nur noch eine Rahmenvorschrift. Damit wird der Änderung von Art. 75 GG durch das 42. Gesetz zur Änderung des Grundgesetzes vom 27.10.1994 (BGBl. I S. 3146) Rechnung getra-gen. Da die Ausgestaltung der zu den in Absatz 1 genannten Zwecken erfolgenden redaktionellen Datenverarbeitung mitprägend für die Gestaltung der Rechtsverhältnisse der Presse ist und somit nur in die Rahmenkompetenz des Bundes fällt, gelten insoweit die übrigen BDSG-Regelungen nicht. Die Vorschrift, die damit auf dem Gebiet des redaktionellen Datenschutzes lex specialis zu § 1 Abs. 2 Nr. 3 ist, enthält dementsprechend auch keine unmittelbar geltenden Regelungen, sondern gibt für die in die Zuständigkeit der Länder fallende Umsetzung lediglich den Mindeststandard der in der Rechtsprechung seit dem Volkszählungsurteil des Bundesverfassungsgerichts (BVerfGE 65, 1) geforderten datenschutzrechtlichen Regelungen im Bereich der Medien unter Berücksichtigung des aufgrund von Artikel 9 der Richtlinie bestehenden Änderungsbedarfs vor.* *In Umsetzung von Artikel 9 der Richtlinie erweitert Absatz 1 den Anwendungsbereich der Datenschutzbestimmungen im Rahmen der Verarbeitung personenbezogener Da-ten durch Medien. Artikel 9 der Richtlinie sieht keine Ausnahme von den Vorschriften des Dritten Kapitels der Richtlinie – Rechtsbehelfe, Haftung und Sanktionen – vor. Die Regelung zur Haftung war daher in die Regelung des § 41 einzubeziehen. Entspre-chendes gilt für das Fünfte Kapitel der Richtlinie – Verhaltensregeln zur Förderung der Durchführung datenschutzrechtlicher Regelungen –.* *Der Deutsche Presserat wird im Wege der Selbstregulierung ergänzende Regelungen treffen. Inhalte dieser Selbstregulierung werden insbesondere die Erarbeitung von – nicht notwendigerweise auf den Anwendungsbereich der §§ 5 und 9 beschränkten – Verhaltensregeln und Empfehlungen, eine regelmäßige Berichterstattung zum redak-tionellen Datenschutz sowie die Schaffung eines Beschwerdeverfahrens sein, das Be-troffenen die Möglichkeit einer presseinternen Überprüfung beim Umgang mit perso-nenbezogenen Daten eröffnet.* *Dieses Konzept ist zu begrüßen, da es in besonderer Weise geeignet erscheint, den Datenschutz im Medienbereich weiter zu verstärken. Insbesondere vor diesem Hintergrund besteht nach Auffassung des Bundes keine Veranlassung für die Länder, über die im Gesetz genannten Vorgaben hinausgehende Regelungen zu treffen.*
(2) Führt die journalistisch-redaktionelle Verarbeitung oder Nutzung personenbezogener Daten durch die Deutsche Welle zur Veröffentlichung von Gegendarstellungen	(2) Führt die journalistisch-redaktionelle Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durch die Deutsche Welle zur Veröffentlichung von Ge-	

des Betroffenen, so sind diese Gegendarstellungen zu den gespeicherten Daten zu nehmen und für dieselbe Zeitdauer aufzubewahren wie die Daten selbst.	gendarstellungen des Betroffenen, so sind diese Gegendarstellungen zu den gespeicherten Daten zu nehmen und für dieselbe Zeitdauer aufzubewahren wie die Daten selbst.	
(3) [1]Wird jemand durch eine Berichterstattung der Deutschen Welle in seinem Persönlichkeitsrecht beeinträchtigt, so kann er Auskunft über die der Berichterstattung zugrundeliegenden, zu seiner Person gespeicherten Daten verlangen. [2]Die Auskunft kann verweigert werden, soweit aus den Daten auf die Person des Verfassers, Einsenders oder Gewährsmannes von Beiträgen, Unterlagen und Mitteilungen für den redaktionellen Teil geschlossen werden kann. [3]Der Betroffene kann die Berichtigung unrichtiger Daten verlangen.	(3) [1]Wird jemand durch eine Berichterstattung der Deutschen Welle in seinem Persönlichkeitsrecht beeinträchtigt, so kann er Auskunft über die der Berichterstattung zugrundeliegenden, zu seiner Person gespeicherten Daten verlangen. [2]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. [3]Der Betroffene kann die Berichtigung unrichtiger Daten verlangen.	*Die Neufassung passt die Auskunftsregelung an den Stand neuerer Vorschriften an (vgl. § 17 Abs. 3 ZDF-Staatsvertrag oder § 16 Abs. 3 Mediendienstestaatsvertrag).*
(4) [1]Im übrigen gelten für die Deutsche Welle von den Vorschriften dieses Gesetzes die §§ 5 und 9. [2]Anstelle der §§ 24 bis 26 gilt § 42, auch soweit es sich um Verwaltungsangelegenheiten handelt.	(4) [1]Im übrigen gelten für die Deutsche Welle von den Vorschriften dieses Gesetzes die §§ 5, 7, 9 und 38a. [2]Anstelle der §§ 24 bis 26 gilt § 42, auch soweit es sich um Verwaltungsangelegenheiten handelt.	*Der Kreis der auf die Deutsche Welle anwendbaren Vorschriften des Bundesdatenschutzgesetzes war nach Maßgabe des Artikels 9 der Richtlinie zu erweitern.*

§ 42 a.F.	§ 42 n.F.	
Datenschutzbeauftragter der Deutschen Welle	Datenschutzbeauftragter der Deutschen Welle	
(1) [1]Die Deutsche Welle bestellt einen Beauftragten für den Datenschutz, der an die Stelle des Bundesbeauftragten für den Datenschutz tritt. [2]Die Bestellung erfolgt auf Vorschlag des Intendanten durch den Verwaltungsrat für die Dauer von vier Jahren, wobei Wiederbestellungen zulässig sind. [3]Das Amt eines Beauftragten für den Datenschutz kann neben anderen Aufgaben innerhalb der Rundfunkanstalt wahrgenommen werden.	(1) [1]Die Deutsche Welle bestellt einen Beauftragten für den Datenschutz, der an die Stelle des Bundesbeauftragten für den Datenschutz tritt. [2]Die Bestellung erfolgt auf Vorschlag des Intendanten durch den Verwaltungsrat für die Dauer von vier Jahren, wobei Wiederbestellungen zulässig sind. [3]Das Amt eines Beauftragten für den Datenschutz kann neben anderen Aufgaben innerhalb der Rundfunkanstalt wahrgenommen werden.	
(2) [1]Der Beauftragte für den Datenschutz kontrolliert die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz. [2]Er ist in Ausübung dieses Amtes unabhängig und nur dem Gesetz unterworfen. [3]Im übrigen untersteht er der Dienst- und Rechtsaufsicht des Verwaltungsrates.	(2) [1]Der Beauftragte für den Datenschutz kontrolliert die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz. [2]Er ist in Ausübung dieses Amtes unabhängig und nur dem Gesetz unterworfen. [3]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.	(3) Jedermann kann sich entsprechend § 21 Satz 1 an den Beauftragten für den Datenschutz wenden.	
(4) [1]Der Beauftragte für den Datenschutz erstattet den Organen der Deutschen Wel-le alle zwei Jahre, erstmals zum 1. Januar 1994 einen Tätigkeitsbericht. [2]Er erstattet darüber hinaus besondere Berichte auf Beschluß eines Organes der Deutschen Welle. [3]Die Tätigkeitsberichte übermittelt der Beauftragte auch an den Bundesbeauftragten für den Datenschutz.	(4) [1]Der Beauftragte für den Datenschutz erstattet den Organen der Deutschen Wel-le alle zwei Jahre, erstmals zum 1. Januar 1994 einen Tätigkeitsbericht. [2]Er erstattet darüber hinaus besondere Berichte auf Beschluss eines Organes der Deutschen Welle. [3]Die Tätigkeitsberichte übermittelt der Beauftragte auch an den Bundesbeauftragten für den Datenschutz.	
(5) [1]Weitere Regelungen entsprechend den §§ 23 bis 26 trifft die Deutsche Welle für ihren Bereich. [2]§ 18 bleibt unberührt.	(5) [1]Weitere Regelungen entsprechend den §§ 23 bis 26 trifft die Deutsche Welle für ihren Bereich. [2]Die § 4f und 4g bleiben un-	*Die Änderungen in Absatz 5 Satz 2 sind Folgeänderungen im Zusammenhang mit der Schaffung einheitlicher Vorschriften für den internen Beauftragten für den Datenschutz (§§ 4 f und 4 g). Diese Regelungen über den internen Beauftragten für den Daten-schutz,*

	berührt.	*die erstmals auch für den behördlichen Bereich Anwendung finden, gelten da-mit ausdrücklich im Bereich der Deutschen Welle. Hierdurch erfährt insbesondere auch der Datenschutzbeauftragte der Deutschen Welle eine deutliche Aufwertung.*
Fünfter Abschnitt **Schlussvorschriften**	**Fünfter Abschnitt** **Schlussvorschriften**	
§ 43 a.F.	§ 43 n.F.	
Strafvorschriften	Bußgeldvorschriften	
(1) Wer unbefugt von diesem Gesetz geschützte personenbezogene Daten, die nicht offenkundig sind, 1. speichert, verändert oder übermittelt, 2. zum Abruf mittels automatisierten Verfahrens bereithält oder 3. abruft oder sich oder einem anderen aus Dateien verschafft, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.	(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig 1. entgegen § 4d Abs. 1, auch in Verbindung mit § 4e Satz 2, eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht, 2. entgegen § 4f Abs. 1 Satz 1 oder 2, jeweils auch in Verbindung mit Satz 3 und 6, einen Beauftragten für den Datenschutz nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig bestellt, 3. entgegen § 28 Abs. 4 Satz 2 den Betroffenen nicht, nicht richtig oder nicht rechtzeitig unterrichtet oder nicht sicherstellt, dass der Betroffene Kenntnis erhalten kann, 4. entgegen § 28 Abs. 5 Satz 2 personenbezogene Daten übermittelt oder nutzt, 5. entgegen § 29 Abs. 2 Satz 3 oder 4 die dort bezeichneten Gründe oder die Art und Weise ihrer glaubhaften Darlegung nicht aufzeichnet, 6. entgegen § 29 Abs. 3 Satz 1 perso-	*Der Formulierung „von diesem Gesetz geschützte“ in Absatz 1 vor Nummer 1 sowie in Absatz 2 Nr. 1 kam kein eigenständiger Regelungsinhalt zu. Er war daher zu streichen. Die Änderungen in Absatz 1 Nr. 1 passen die Terminologie der Strafvorschriften an die des übrigen Bundesdatenschutzgesetzes an.* *Die Änderung der Verweise in Absatz 2 Nr. 2 ist eine Folgeänderung im Zusammen-hang mit der Einfügung eines neuen Absatzes 3 in § 29.* *Die Änderung der Verweise in Absatz 2 Nr. 3 ist eine Folgeänderung im Zusammen-hang mit der Aufhebung von § 40 Abs. 2 a.F.* *Die Änderung der Verweise in Absatz 1 Nr. 2 ist eine Folgeänderung im Zusammen-hang mit der Aufhebung von § 32 sowie mit der Schaffung der neuen Vorschriften der §§ 4 d und 4 e.* *Die Änderung ist eine Folgeänderung im Zusammenhang mit der Einfügung eines neuen Absatzes 5 in § 35.* *Die Änderung des Verweises in Absatz 1 Nr. 5 ist eine Folgeänderung im Zusammenhang mit der Aufhebung von § 36 sowie mit der Schaffung der neuen Vorschrift des § 4 f.* *Sachlich zuständig für die Durchführung des Ordnungswidrigkeitenverfahrens ist nach § 36 Abs. 1 Nr. 2 b OwiG der fachlich zuständige Bundesminister, soweit das Gesetz von Bundesbehörden ausgeführt wird.* ***Der Bundesrat schlägt vor, die Straf- und Bußgeldvorschriften zu überarbeiten und dabei insbesondere den Grundtatbestand der bisherigen Strafvorschrift in den Ordnungswidrigkeitenkatalog zu überführen. Er begründet dies im Wesentlichen damit, dass der Grundtatbestand der Strafvorschrift geringe praktische Bedeutung habe. Die Lösung, insoweit die Verfolgung als Ordnungswidrigkeit zu ermöglichen, gestatte den zuständigen Kontrollbehörden eine flexiblere Reaktion als sie nach geltendem Recht möglich sei.***

	nenbezogene Daten in elektronische oder gedruckte Adress-, Rufnummern-, Branchen- oder vergleichbare Verzeichnisse aufnimmt,	***Der Bundesrat hat außerdem vorgeschlagen, den Bußgeldkatalog zu erweitern.***
	7. entgegen § 29 Abs. 3 Satz 2 die Übernahme von Kennzeichnungen nicht sicherstellt,	***Die Vorschläge des Bundesrats werden zum Anlass genommen, die Straf- und Bußgeldvorschrift insgesamt zu überarbeiten, zu straffen und widerspruchsfrei auszugestalten. Die Sanktionsbestände werden nur in begrenztem Umfang erweitert. Hierfür spricht, dass das Gesamtgefüge der Gebots- und Verbotsnorm des BDSG im Zuge der geplanten grundlegenden Reform des Datenschutzrechts ohnehin einer Prüfung zu unterziehen ist, bei der auch die Notwendigkeit der weiteren Verwendung von Blankettvorschriften zu untersuchen sein wird. Gegenwärtig bedarf der – um den bisherigen Grundtatbestand der Strafvorschriften ergänzte – Bußgeldkatalog nur insoweit der Anpassung, als mit dem Gesetzentwurf neue Handlungsge- und -verbote neu eingeführt werden oder ergänzt wurden, ohne dass diese nicht bereits von § 43 Abs. 2 Nr. 1 bis 3 erfasst werden. Dies betrifft § 43 Abs. 1 Nr. 3 und 4 sowie Nr. 6 und 7, die eine Verletzung der Vorschriften § 28 Abs. 3 und Abs. 4 (neu) sanktionieren.***
		In der Übersicht wirkt sich gegenüber der Fassung des Regierungsentwurfs die Umstellung wie folgt aus:
	8. entgegen § 33 Abs. 1 den Betroffenen nicht, nicht richtig oder nicht vollständig benachrichtigt,	
	9. entgegen § 35 Abs. 6 Satz 3 Daten ohne Gegendarstellung übermittelt,	
	10. entgegen § 38 Abs. 3 Satz 1 oder Abs. 4 Satz 1 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder eine Maß-nahme nicht duldet oder	
	11. einer vollziehbaren Anordnung nach § 38 Abs. 5 Satz 1 zuwiderhandelt.	
(2) Ebenso wird bestraft, wer	(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig	
1. die Übermittlung von durch dieses Gesetz geschützten personenbezogenen Daten, die nicht offenkundig sind, durch unrichtige Angaben erschleicht,	1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,	
2. entgegen § 16 Abs. 4 Satz 1, § 28 Abs. 4 Satz 1, auch in Verbindung mit	2. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, zum	***Für diese Neufassung sind folgende Erwägungen maßgeblich:***

Fassung Regierungsentwurf	Nach Umstellung
§ 44 Abs. 1 (Bußgeldvorschr.)	§ 43 Abs. 1 (Bußgeldvorschr.)
Nr. 2	Nr. 1
Nr. 5	Nr. 2
	Nr. 3 (neu)
	Nr. 4 (neu)
Nr. 1	Nr. 5
	Nr. 6 (neu)
	Nr. 7 (neu)
Nr. 3	Nr. 8
Nr. 4	Nr. 9
Nr. 6	Nr. 10
Nr. 7	Nr. 11

Fassung Regierungsentwurf	Nach Umstellung
§ 43 (Strafvorschr.)	§ 43 Abs. 2 (Bußgeldvorschr.)
Abs. 1 Nr. 1	Nr. 1
" Nr. 2	Nr. 2
" Nr. 3	Nr. 3
Abs. 2 Nr. 1	Nr. 4
" Nr. 2	Nr. 5
" Nr. 3	Nr. 6
§ 43 Abs. 3 (Strafvorschr.)	§ 44 Abs. 1 (Strafvorschr.)
§ 43 Abs. 4 (Strafvorschr.)	§ 44 Abs. 2 (Strafvorschr.)

§ 29 Abs. 3, § 39 Abs. 1 Satz 1 oder § 40 Abs. 1 die übermittelten Daten für andere Zwecke nutzt, indem er sie an Dritte weitergibt, oder

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

(3) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

(4) Die Tat wird nur auf Antrag verfolgt.

Abruf mittels automatisierten Verfahrens bereithält,

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

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

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

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

(3) Die Ordnungswidrigkeit kann im Falle des Absatzes 1 mit einer Geldbuße bis zu fünfzigtausend Deutsche Mark, in den Fällen des Absatzes 2 mit einer Geldbuße bis zu fünfhunderttausend Deutsche Mark geahndet werden.

Im Gegensatz zum geltenden Recht, in dem die Straf- und Bußgeldvorschriften voneinander unabhängig normiert sind, bilden sie nach dem Konzept des Bundesrates unechte Mischtatbestände. Die Straf- und Bußgeldvorschriften stimmen im Grundtatbestand überein; bei den Straftatbeständen treten zu dem Grundtatbestand weitere Merkmale hinzu, nämlich das Handeln gegen Entgelt oder in Bereicherungs- oder Schädigungsabsicht. Diese enge Verknüpfung von Straf- und Bußgeldvorschriften ist in der Formulierung der Strafvorschriften hervorzuheben. Hierzu wird in den Strafvorschriften auf die Bußgeldnormen Bezug genommen, die im Grundtatbestand mit den Strafvorschriften übereinstimmen. Diese Fassung der Strafvorschriften entspricht der üblichen Rechtsetzungstechnik, führt zu einer wesentlichen Straffung der Strafnormen und vermeidet Unstimmigkeiten zwischen den Strafvorschriften und den zugehörigen Bußgeldvorschriften. Zur Vermeidung einer – rechtstechnisch ungewöhnlichen – Verweisung auf nachfolgende Vorschriften werden – wie im Nebenstrafrecht üblich – zunächst in § 43 BDSG die Bußgeldvorschriften und sodann in § 44 BDSG die Strafvorschriften normiert.

Entsprechend der üblichen Handhabung im Nebenstrafrecht folgt die Reihenfolge der Bußgeldvorschriften der numerischen Abfolge der bewehrten verwaltungsrechtlichen Vorschriften.

Bei § 43 Abs. 2 Nr. 6 handelt es sich materiell um die Strafnorm des geltenden § 43 Abs. 2 Nr. 3 BDSG, die entsprechend dem Vorschlag des Bundesrates nunmehr im Grundtatbestand nur noch eine Ordnungswidrigkeit sein soll. Dem Vorschlag des Bundesrats, diese Vorschrift als neue Nummer 11 in Absatz 1 der Bußgeldvorschrift einzustellen, wird nicht gefolgt. Es erscheint nicht vertretbar, eine Strafvorschrift in eine Bußgeldvorschrift umzuwandeln, die Verstöße lediglich mit Geldbuße bis zu 50.000 DM (vgl. § 43 Abs. 3 BDSG) bedroht. Zudem bestünden unter dem Gesichtspunkt der Verhältnismäßigkeit Bedenken, eine – ge-messen an der Bußgelddrohung – relativ geringfügige Ordnungswidrigkeit durch weitere Tatbestandsmerkmale zu einer Strafvorschrift zu "qualifizieren". Bei unechten Mischtatbeständen muss die sachliche Nähe zwischen Straf- und Bußgeldvorschrift auch in der Relation zwischen den Sanktionen zum Ausdruck kommen: Während für die Strafvorschrift eine Strafdrohung im unteren Bereich vorzusehen ist, sollte sich die Bußgeldnorm durch eine Bußgelddrohung auszeichnen, die den Regelrahmen des § 17 Abs. 1 OWiG deutlich übertrifft. Dies wird üblicherweise aber erst bei einem Bußgeldrahmen angenommen, der 100.000 DM erreicht oder übersteigt. Der neue Bußgeldtatbestand ist deshalb nicht in Absatz 1, sondern in Absatz 2 der Bußgeldvorschrift einzustellen.

Durch die Formulierung „allgemein zugänglich“ in § 43 Nr. 1 bis 3 (vgl. die zu § 10 Abs. 5 eingeführte Definition) wird sichergestellt, dass bei Vorliegen der sonstigen Voraussetzungen eine Ahndung nur in denjenigen Fällen ausgschlossen ist, in de-

		nen es sich um Daten handelt, die von jedermann zur Kenntnis genommen werden können.
§ 44 a.F.	§ 44 n.F.	
Bußgeldvorschriften	Strafvorschriften	
(1) Ordnungswidrig handelt, wer vorsätz-lich oder fahrlässig	(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.	
1. entgegen § 29 Abs. 2 Satz 3 oder 4 die dort bezeichneten Gründe oder die Art und Weise ihrer glaubhaften Darlegung nicht aufzeichnet, 2. entgegen § 32 Abs. 1, auch in Verbindung mit Absatz 4, eine Meldung nicht oder nicht rechtzeitig erstattet oder entgegen § 32 Abs. 2, auch in Verbindung mit Absatz 4, bei einer solchen Meldung die erforderlichen Angaben nicht, nicht richtig oder nicht vollständig mitteilt, 3. entgegen § 33 Abs. 1 den Betroffenen nicht, nicht richtig oder nicht vollständig benachrichtigt, 4. entgegen § 35 Abs. 5 Satz 3 Daten ohne Gegendarstellung übermittelt, 5. entgegen § 36 Abs. 1 einen Beauftragten für den Datenschutz nicht oder nicht rechtzeitig bestellt, 6. entgegen § 38 Abs. 3 Satz 1 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder entgegen § 38 Abs. 4 Satz 4 den Zutritt zu den Grundstücken oder Geschäftsräumen oder die Vornahme von Prüfungen oder Besichtigungen oder die Einsicht in geschäftliche Unterlagen	(2) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind der Betroffene, die verantwortliche Stelle, der Bundesbeauftragte für den Datenschutz und die Aufsichtsbehörde."	*Der Zusatz in Absatz 4* [jetzt § 44 Abs. 2]*ist durch die Ergänzung des § 23 Abs. 5 durch einen Satz 7 erforderlich geworden. Danach steht dem Bundesbeauftragten für den Datenschutz eine Anzeigebefugnis in Umsetzung des Artikels 28 Abs. 3, 3. Spiegelstrich der Richtlinie zu. Entsprechendes gilt nach § 38 Abs. 1 Satz 7 für die Aufsichtsbehörden der Länder für den nicht-öffentlichen Bereich. Die Aufnahme der verantwortlichen Stelle ist sachgerecht, damit sich diese gegen einen Missbrauch der von ihr gespeicherten Daten zur Wehr setzen kann.*

nicht duldet, oder 7. einer vollziehbaren Anordnung nach § 38 Abs. 5 Satz 1 zuwiderhandelt. (2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Deutsche Mark geahndet werden.		
Sechster Abschnitt **Übergangsvorschriften**	**Sechster Abschnitt** **Übergangsvorschriften**	
	§ 45 n.F. Laufende Verwendungen	
	[1]Erhebungen, Verarbeitungen oder Nutzungen personenbezogener Daten, die am ... [einsetzen: Tag nach der Verkündung dieses Gesetzes] bereits begonnen haben, sind binnen drei Jahren nach diesem Zeitpunkt mit den Vorschriften dieses Gesetzes in Übereinstimmung zu bringen. [2]So-weit 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 ... [einsetzen: Tag nach der Verkündung dieses Gesetzes] bereits begonnen haben, binnen fünf Jahren nach diesem Zeitpunkt mit den Vorschriften dieses Gesetzes in Übereinstimmung zu bringen.	*Die Vorschrift setzt Artikel 32 Abs. 2 der Richtlinie um. Er gestattet einen Anpassungszeitraum von maximal drei Jahren ab Inkrafttreten des Gesetzes für solche Erhebun-gen, Verarbeitungen oder Nutzungen personenbezogener Daten, die zum Zeitpunkt des Inkrafttretens der Änderungen des Bundesdatenschutzgesetzes bereits begonnen haben.* *§ 45 gilt auch in den Rechtsbereichen, die nicht in den Anwendungsbereich der Richt-linie fallen, soweit die Vorschriften des BDSG in den jeweiligen bereichsspezifischen Gesetzen zur Anwendung gelangen. Hierfür enthält Satz 2 eine Sonderregelung.* ***Die Änderung des § 45 ist – nach Änderung des § 4b – redaktioneller Natur.***
	§ 46 n.F.	

Weitergeltung von Begriffsbestimmungen	
(1) [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 Merkma-len geordnet, umgeordnet und ausgewertet werden kann (nicht automatisier-te Datei). [2]Nicht hierzu gehören Akten und Aktensammlungen, es sei denn, dass sie durch automatisierte Verfahren umgeordnet und ausgewertet werden können.	*Da es aus zeitlichen Gründen nicht möglich ist, das gesamte bereichsspezifische Datenschutzrecht bereits in der 1. Gesetzgebungsstufe an die neue Terminologie des BDSG anzupassen, wird angeordnet, dass die bisherigen Definitionen der Begriffe Da-tei, Akte und Empfänger zunächst weitergelten sollen. Es ist beabsichtigt, in der 2. Novellierungsstufe die Anpassung des bereichsspezifischen Datenschutzrechts an die Richtlinie umfassend zu überprüfen.* *Absatz 1 entspricht § 3 Abs. 2 a.F., Absatz 2 § 3 Abs. 3 a.F. und Absatz 3 § 3 Abs. 9 a.F.*
(2) [1]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 un-terfällt; dazu zählen auch Bild- und Tonträger. [2]Nicht hierunter fallen Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen.	
(3) [1]Wird in besonderen Rechtsvorschriften des Bundes der Begriff Empfänger verwendet, ist Empfänger jede Person oder Stelle außerhalb der verantwortlichen Stelle. [2]Empfänger sind nicht der Betroffe-ne sowie Personen und Stellen, die im In-land, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Ver-	***Hinsichtlich des § 46 Abs. 3*** [Einbeziehung der EWR-Vertragsstaaten] ***wird auf die Begründung zu § 1 Abs. 5 und § 3 Abs. 8 verwiesen.***

	tragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.	
Anlage (zu § 9 Satz 1) a.F.	Anlage (zu § 9 Satz 1) n.F.	
Werden personenbezogene Daten automatisiert verarbeitet, sind Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind,	[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. [2]Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,	*Die Anlage zu § 9 wurde gestrafft (Einfügung von Nummer 10 a.F. in Satz 1 vor Nummer 1, Zusammenführung von Nummern 2, 3 und 5 a.F. als Teil von Nummer 3), um die Anforderungen der Richtlinie ergänzt (insbesondere Nummer 7 n.F.), sprachlich überarbeitet (Nummern 1 bis 5) sowie den heutigen Gegebenheiten der Informations- und Kommunikationstechnik angepasst (Nummern 4 und 5). Allgemein gilt, dass Schutzzweck und Aufwand maßgeblich für die Festlegung der Einzelmaßnahmen sind, d.h. dass Einzelmaßnahmen so gewählt werden müssen, dass der Schutz der einzel-nen gespeicherten Daten konkret gewährleistet wird.*
		Im Einzelnen:
1. Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zugangskontrolle),	1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),	*1. Die Erweiterung um den Begriff der Nutzung in Satz 1, vor Nummer 1, sowie in Nummer 1 beruht auf Artikel 3 Abs. 1 in Verbindung mit Artikel 2 Buchstabe b der Richtlinie.*
2. zu verhindern, daß Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle),	2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),	*2. Die Einfügung „Datenkategorien“ in Satz 1, vor Nummer 1, ist eine Anpassung an die Terminologie der Richtlinie. Auf Artikel 19 Abs. 1 Buchstabe c der Richtlinie so-wie die Begründung zu § 4 e Satz 1 Nr. 5 wird verwiesen.*
3. die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten zu verhindern (Speicherkontrolle),	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),	*Zugang im Sinne der Nummer 2 (Nummer 4 a.F.) erfasst das Eindringen in das EDV-System selbst seitens unbefugter (externer) Personen.*
4. zu verhindern, daß Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können (Benutzerkontrolle),	4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger	*3. Bei den Nummern 1, 2 und 3 (Nummern 1, 2, 3, 4 und 5 a.F.) wurde der gesetzliche Wortlaut der gebräuchlichen informationstechnischen Terminologie angepasst: Zu-tritt im Sinne der Nummer 1 ist ausschließlich räumlich zu verstehen, erfasst daher den räumlichen Zutritt durch unbefugte (externe) Personen. Nummer 1 a.F. war demgegenüber sprachlich unklar und gab Anlass zu unterschiedlichen Interpretationen.*
5. zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle),		*Durch den Verzicht auf die Formulierung „mit Hilfe von Einrichtungen zur Datenübertragung“ in Nummer 2 wurde gegenüber der bisherigen Nummer 4 a.F. der Anwendungsbereich neben dem bereits erfassten Schutz des Zugangs über Datenübertragungseinrichtungen auf den Schutz des lokalen Zugangs zum System erweitert. Zugriff im Sinne der Nummer 3 schließlich erfasst die Tätigkeit innerhalb des EDV-Systems durch einen grundsätzlich Berechtigten außerhalb seiner Berechtigung. Nummer 3 entspricht in ihrem ersten Teil vollständig Nummer 5 a.F. und beinhaltet in*

6. zu gewährleisten, daß überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können (Übermittlungskontrolle),	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),	*ihrem zweiten Teil eine teilweise Zusammenfassung von Nummern 2 und 3 a.F.; die Überschneidungen dieser Nummern der alten Fassung werden beseitigt. Auf den Begriff „Löschung“ in Nummern 3 und 9 a.F. konnte verzichtet werden, da er im informationstechnischen Sinn vom Begriff „Veränderung“ mit umfasst wird.*
7. zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle),	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),	*4. Nummer 4 fasst sämtliche Aspekte der Weitergabe personenbezogener Daten, also elektronische Übertragung, Datenträgertransport und Übermittlungskontrolle, unter dem Begriff „Weitergabekontrolle“ zusammen. Zu ergänzen war Nummer 4 um den Begriff der „elektronischen Übertragung“. Der zweite Teil von Nummer 4 entspricht im Wesentlichen Nummer 6 a.F.*
8. zu gewährleisten, daß personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),	6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),	*Die in der neuen Fassung von Nummer 4, zweiter Teil durch die vorgenommene Änderung („vorgesehen“ anstelle von „werden können“) gegenüber Nummer 6 a.F. erfolgte Eingrenzung ist angesichts der technischen Entwicklung – weitgehend unbegrenzte Möglichkeit zur Datenübertragung als Normalfall – notwendig.*
9. zu verhindern, daß bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle),	7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),	*5. Nummer 5 stellt im Gegensatz zur bisherigen Fassung (Nummer 7 a.F.) nicht mehr in erster Linie auf die eingegebenen Daten ab („welche“), sondern maßgeblich auf den Zugang („ob“). Dies war erforderlich, da die Praxis erwiesen hat, dass die bishe-rige Fassung überzogene, nicht praktikable Anforderungen stellte. Gleichzeitig wur-de der Anwendungsbereich der Nummer 5 um die nachträgliche Überprüfung und Feststellung der Veränderung oder Entfernung ergänzt.*
10. die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).	8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	*6. Nummer 6 entspricht unverändert Nummer 8 a.F.*
		7. Die in Nummer 7 neu aufgenommene Verfügbarkeitskontrolle beruht auf Artikel 17 Abs. 1 der Richtlinie. Schutz vor zufälliger Zerstörung oder Verlust meint beispielsweise Schutz vor Wasserschäden, Blitzschlag oder Stromausfall. Beispiel für eine insoweit zu treffende Sicherungsmaßnahme ist etwa das Erstellen zusätzlicher Sicherungskopien, die an besonders geschützten Orten gelagert werden.
		8. Die Regelung in Nummer 8 beinhaltet in Anlehnung an die Regelung des § 4 Abs. 2 Nr. 4 TDDSG ein grundsätzliches Trennungsgebot zu unterschiedlichen Zwecken erhobener Daten. Dieses Trennungsgebot findet in den Fällen eine Einschränkung, in denen ein Informationssystem daraufhin konzipiert ist, dass gesetzlich im Regel-fall zugelassenen Zweckänderungen Rechnung getragen werden soll.