NOVELLIERUNG BDSG (STAND: 16. März 2000)

Erster Abschnitt

Allgemeine und gemeinsame Bestimmungen

§ 1 a.F.	§ 1 n.F.	***Begründung:***
Zweck und Anwendungsbereich des Gesetzes	Zweck und Anwendungsbereich des Gesetzes	*Zu Absatz 2 Nr. 3:*
(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.	(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.	*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 übrigen Datenverarbeitungen durch nicht-öffentliche Stellen werden daher – soweit es sich um automatisierte Verarbeitungen oder um (nicht-automatisierte) Dateien handelt (vgl. hierzu die Begründung zu § 3 Abs. 2) - vom Anwendungsbereich der Richtlinie erfaßt. Die Vorschrift des Absatzes 2 Nr. 3 war dementsprechend zu ändern.*
(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 Landesgesetz 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 Landesgesetz geregelt ist und soweit sie a) Bundesrecht ausführen oder b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt,	
3. nicht-öffentliche Stellen, soweit sie die Daten 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 <u>nicht-automatisierten</u> Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.**	

§ 1 a.F. (Forts.)	§ 1 n.F. (Forts.)	***Begründung:***
(3) Bei der Anwendung dieses Gesetzes gelten folgende Einschränkungen: 1. Für automatisierte Dateien, die ausschließlich aus verarbeitungstechnischen Gründen vorübergehend erstellt und nach ihrer verarbeitungstechnischen Nutzung automatisch gelöscht werden, gelten nur die §§ 5 und 9. 2. **1**Für nicht-automatisierte Dateien, deren personenbezogene Daten nicht zur Übermittlung an Dritte bestimmt sind, gelten nur die §§ 5, 9, 39 und 40. **2**Außerdem gelten für Dateien öffentlicher Stellen die Regelungen über die Verarbeitung und Nutzung personenbezogener Daten in Akten. **3**Werden im Einzelfall personenbezogene Daten übermittelt, gelten für diesen Einzelfall die Vorschriften dieses Gesetzes uneingeschränkt. (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. (5) Die Vorschriften dieses Gesetzes gehen denen des Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.	(**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. (**4**) Die Vorschriften dieses Gesetzes gehen denen des Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden. **(5) Dieses Gesetz findet keine Anwendung, sofern eine in einem anderen Mitgliedstaat der Europäischen Union belegene verantwortliche Stelle personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt, es**	*Zu Absatz 3:* *Absatz 3 war in Umsetzung von Artikel 3 Abs. 1 der Richtlinie aufzuheben, da die Richtlinie eine entsprechende Einschränkung des Anwendungsbereichs nicht vorsieht.* *zu Absatz 5:* *Artikel 4 der Richtlinie geht hinsichtlich des Anwendungsbereichs nationalen Datenschutzrechts im grenzüberschreitenden Datenverkehr - anders als das derzeit geltende Bundesdatenschutzgesetz - im Grundsatz nicht vom Territorial-prinzip, sondern vom Sitzprinzip aus. Danach richtet sich das insoweit anzuwendende nationale Recht nicht nach dem Ort der Ver-arbeitung, 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, Verarbeitung oder Nutzung personenbezogener Daten durch diese Niederlassung gilt dann das nationale Datenschutz-recht des Landes, in dem sie belegen ist.*

	§ 1 n.F. (Forts.) **sei denn, dies erfolgt durch eine Niederlassung im Inland. Dieses Gesetz findet Anwendung, sofern eine außerhalb der Europäischen Union belegene verantwortliche Stelle personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt. Soweit die verantwortliche Stelle nach den Vorschriften dieses Gesetzes zu nennen ist, sind auch Angaben über im Inland ansässige Vertreter zu machen. Die Sätze 2 und 3 gelten nicht, sofern Datenträger nur zum Zwecke des Transits durch das Inland eingesetzt werden. § 38 Abs. 1 Satz 1 bleibt unberührt.**	***Begründung (Forts.):*** *Diese Regelung der Richtlinie stellt einen Kompromiß dar zwischen den Belangen der Wirtschaft einerseits: Diese soll ihr gewohntes nationales Datenschutzrecht "exportieren" 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 maßgeblich." Zur Erläuterung des Begriffs Niederlassung kann auf die Definition der Niederlassung in § 42 Abs. 2 Gewerbeordnung verwiesen werden. Dieser zufolge ist eine Niederlassung 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 Ausnahme - das*

§ 1 a.F.	§ 1 n.F.	***Begründung (Forts.):***
		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 Drittland 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.*

§ 2 a.F. Öffentliche und nicht-öffentliche Stellen (1) **1**Öffentliche Stellen des Bundes sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform. **2**Als öffentliche Stellen gelten die aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange ihnen ein ausschließliches Recht nach dem Postgesetz zusteht. (2) Öffentliche Stellen der Länder sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Landes, einer Gemeinde, eines Gemeindeverbandes und sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform. (3) **1**Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder, die Aufgaben der öffentlichen Verwaltung wahrnehmen, gelten ungeachtet der Beteiligung nicht-öffentlicher Stellen als öffentliche Stellen des Bundes, wenn 1. sie über den Bereich eines Landes hinaus tätig werden oder 2. dem Bund die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht. **2**Andernfalls gelten sie als öffentliche Stellen der Länder. (4) **1**Nicht-öffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Absätze 1 bis 3 fallen. **2**Nimmt eine nicht-öffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.	Hinweis: Die Vorschrift bleibt unverändert.	

§ 3 a.F. Weitere Begriffsbestimmungen	§ 3 n.F. Weitere Begriffsbestimmungen	***Begründung:***
(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).	*Zu Absatz 2:* *Während für das BDSG 1977 noch der Dateibezug für die Anwendbarkeit des Gesetzes maßgebend war, hat das BDSG 1990 grundsätzlich jedes Speichermedium einbezogen und lediglich im nicht-öffentlichen Bereich das Erfordernis des Dateibezugs beibehalten (§ 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, Verarbeitung und Nutzung personenbezogener Daten sowie die nicht-automatisierte Erhebung, Verarbeitung und Nutzung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen.*
(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 aufgebaut ist und nach bestimmten Merkmalen geordnet, umgeordnet und ausgewertet werden kann (nicht-automatisierte Datei). **2**Nicht hierzu gehören Akten und Aktensammlungen, es sei denn, daß sie durch automatisierte Verfahren umgeordnet und ausgewertet werden können.	(2) **Automatisiert im Sinne dieses Gesetzes ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten, wenn sie unter Einsatz von Datenverarbeitungsanlagen durchgeführt wird (automatisierte Verarbeitung). <u>Eine nicht-automatisierte</u> Datei ist jede nicht-automatisierte Sammlung personenbezogener Daten, die ___ <u>gleichartig</u> aufgebaut <u>ist</u> und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann ___.**	*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 <u>(nicht-automatisierten)</u> Datei in Satz 2. Findet hingegen eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten in einer automatisierten Datei statt, ist für die Anwendbarkeit des Bundesdatenschutzgesetzes 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.*
(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.		
(4) Erheben ist das Beschaffen von Daten über den Betroffenen.	(**3**) Erheben ist das Beschaffen von Daten über den Betroffenen.	

§ 3 a.F. (Forts.)	§ 3 n.F. (Forts.)	***Begründung (Forts.):***
(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 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 (Empfänger) in der Weise, daß a) die Daten durch die speichernde Stelle an den Empfänger weitergegeben werden oder b) der Empfänger von der speichernden Stelle 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. (6) Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.	(**4**) **1**Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. **2**Im einzelnen ist, ungeachtet der dabei angewendeten Verfahren: 1. Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung, 2. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten, 3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, daß a) die Daten an den **Dritten** weitergegeben werden oder b) der **Dritte** zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft, 4. Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken, 5. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten. (**5**) Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.	*Zu Satz 2: 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.*

§ 3 a.F. (Forts.)	§ 3 n.F. (Forts.)	***Begründung (Forts.):***
(7) Anonymisieren ist das Verändern personenbezogener Daten derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. (8) Speichernde Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst speichert oder durch andere im Auftrag speichern läßt. (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.	(**6**) Anonymisieren ist das Verändern personenbezogener Daten derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. **(6a) Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.** (**7**) **Verantwortliche** Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst **erhebt, verarbeitet oder nutzt** oder **dies** durch andere im Auftrag **vornehmen** läßt. (**8**) **Empfänger ist jede Person oder Stelle, die Daten erhält.** Dritter ist jede Person oder Stelle außerhalb der **verantwortlichen** Stelle. Dritte sind nicht der Betroffene sowie diejenigen Personen und Stellen, die **im Inland oder** im Geltungsbereich **der Rechtsvorschriften zum Schutz personenbezogener Daten der Mitgliedstaaten der Europäischen Union** personenbezogene Daten im Auftrag **erheben,** verarbeiten oder nutzen. **(9) Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.**	*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, demzufolge die Richtlinie „bei manuellen Verarbeitungen lediglich Dateien erfaßt, nicht jedoch 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 worden: „Der Rat und die Kommission bestätigen, daß sich die Richtlinie nach der derzeitigen Definition in Artikel 2 Buchstabe c nur auf Dateien erstreckt, nicht aber auf Akten; die Kriterien, nach denen sich die Bestandteile einer strukturierten Sammlung personenbezogener Daten bestimmen lassen, sowie die Kriterien, nach denen diese Sammlungen 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*

	<§ 3 Abs. 10 entfällt> ___	***Begründung (Forts.):*** *automatisierten Auswertbarkeit ankommt. Ausschlaggebend ist anstelle dessen, ob eine nicht-automatisierte Datei vorliegt; eine manuelle Auswertbarkeit genügt insoweit.* *Zu Absatz 3:* *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 erfolgt oder wenn die Daten, auf die sich die Verarbeitung bezieht, in Dateien enthalten oder für solche bestimmt sind, die nach bestimmten personenbezogenen Kriterien strukturiert sind, um einen leichten Zugriff zu ermöglichen.„ Maßgeblich für die Einbeziehung 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.* *Zu Absatz 4 Satz 2 Nr. 3:* *Der Begriff der Übermittlung beinhaltet als notwendige Komponenten die Bekanntgabe, die speichernde Stelle als bekanntgebende 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.*

		Begründung (Forts.): *Zu Absatz 6a: 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.* *Zu Absatz 7: 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.* *Zu Absatz 8: 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.* *Zu Absatz 9: Absatz 9 definiert die in Artikel 8 Abs. 1 der Richtlinie bezeichneten besonderen Kategorien personenbezogener Daten.* ___

	§ 3 a n.F. **Datenvermeidung und Datensparsamkeit** **Gestaltung und Auswahl von Datenverarbeitungssysteme n haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.**	***Begründung:*** *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 werden. 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 Bundes 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.	§ 4 n.F.	***Begründung:***
Zulässigkeit der Datenverarbeitung und -nutzung	Zulässigkeit der Daten**erhebung**, -verarbeitung 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 besonderer Umstände eine andere Form angemessen ist. **3**Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben.	**(2) Personenbezogene Daten sind beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn** **1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder** **2.a) die zu erfüllende Verwaltungsaufgabe ihrer Art nach oder der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder** **b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde** **und keine Anhaltspunkte dafür bestehen, daß überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.**	*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 bestimmte Forschungszweck erheblich beeinträchtigt würde. **2**In diesem Fall sind der Hinweis nach Absatz 2 Satz 1 und die Gründe, aus denen sich die erhebliche Beeinträchtigung des bestimmten Forschungszweckes ergibt, schriftlich festzuhalten.		

§ 4 a.F. (Forts.)	§ 4 n.F. (Forts.)	***Begründung (Forts.):***
	(3) Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über **1. die Identität der verantwortlichen Stelle,** **2. die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und** **3. die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muß,** **zu unterrichten.** **Werden personenbezogene Daten beim Betroffenen aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, ist er über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären.** **(4) 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.**	*Absatz 3 modifiziert § 13 Abs. 3 a.F. nach den Voraussetzungen des Artikels 10 der Richtlinie.* *Absatz 4 entspricht § 13 Abs. 4 a.F.*

	§ 4 a n.F. **Einwilligung des Betroffenen** **(1) Die Einwilligung des Betroffenen ist nur wirksam, wenn sie auf dessen freier Entscheidung beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben.** **(2) Im Bereich der wissenschaftlichen Forschung liegt ein besonderer Umstand im Sinne von Absatz 1 Satz 3 auch dann vor, wenn durch die Schriftform der bestimmte Forschungszweck erheblich beeinträchtigt würde. In diesem Fall sind der Hinweis nach Absatz 1 Satz 2 und die Gründe, aus denen sich die erhebliche Beeinträchtigung des bestimmten Forschungszwecks ergibt, schriftlich festzuhalten.**	***Begründung:*** *Absatz 1 Satz 1 berücksichtigt die Voraussetzungen des Artikels 2 Buchstabe h der Richtlinie, wonach die Einwilligung ohne Zwang erfolgen muß. Die Anfügung des Wortes „vorgesehenen„ vor dem Wort „Zweck„ in Satz 2 dient der sprachlichen Verdeutlichung 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 Terminologie der Richtlinie (vgl. hierzu auch die Begründung zu § 4). Die Einfügung der Wörter „soweit nach den Umständen des Einzelfalles erforderlich„ in Satz 2 dient der Umsetzung des Definitionsmerkmals „in Kenntnis der Sachlage„ nach Artikel 2 Buchstabe h der Richtlinie. Die übrigen Anforderungen der Richtlinie sind bereits im Text des § 4 Abs. 2 a.F. verwirklicht, der im Folgenden wiedergegeben wird.* *Absatz 2 entspricht § 4 Abs. 3 a.F.*

	(3) Soweit besondere Arten personenbezogener Daten nach § 3 Abs. 9 erhoben, verarbeitet oder genutzt werden, muß sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.	***Begründung (Forts.):*** *Absatz 3 sieht in Umsetzung des Artikels 8 Abs. 2 Buchstabe a der Richtlinie für die besonderen Arten personenbezogener Daten nach § 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 innerhalb der Mitgliedstaaten der Europäischen Union im Anwendungsbereich von Artikel 3 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 gelten § 15 Abs. 1 und § 16 Abs. 1 sowie §§ 28 bis 30 entsprechend nach Maßgabe der für diese Übermittlung geltenden Gesetze und Vereinbarungen.** **(2) Für die Übermittlung personenbezogener Daten an Stellen der Mitgliedstaaten der Europäischen Union außerhalb des Anwendungsbereichs der in Absatz 1 genannten Richtlinie, an sonstige ausländische Stellen oder an über- oder zwischenstaatliche Stellen gelten § 15 Abs. 1 und § 16 Abs. 1 sowie §§ 28 bis 30 entsprechend nach Maßgabe der für diese Übermittlung geltenden Gesetze und Vereinbarungen. Die Übermittlung unterbleibt, soweit der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat, insbesondere wenn bei den in Satz 1 genannten Stellen ein angemessenes Datenschutzniveau nicht gewährleistet ist. Satz 2 gilt nicht, wenn die Übermittlung zur Erfüllung eigener Aufgaben einer öffentlichen Stelle des Bundes aus zwingenden Gründen der Verteidigung oder der Erfüllung über- oder zwischenstaatlicher Verpflichtungen auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Maßnahmen erforderlich ist.**	***Begründung:*** *Die Vorschrift regelt - anders als § 17 BDSG a.F. - die Übermittlung personenbezogener Daten ins Ausland sowohl für den öffentlichen als auch den nicht-öffentlichen Bereich.* *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.).* *Absatz 2 findet Anwendung bei Übermittlungen an EU-Mitgliedstaaten außerhalb der ersten Säule des EU-Vertrags sowie an Drittländer. Absatz 2 Satz 2 ergänzt § 17 Abs. 1 a.F. um das Erfordernis des angemessenen Datenschutzniveaus im Drittland 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, überflüssig. Die Angemessenheit des Datenschutzniveaus in einem Drittland 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.*

	(3) Die Angemessenheit des Schutzniveaus wird unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen von Bedeutung sind; insbesondere können die Art der Daten, die Zweckbestimmung, die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die für den betreffenden Empfänger geltenden Rechtsnormen sowie die für ihn geltenden Standesregeln und Sicherheitsmaßnahmen herangezogen werden. **(4) In den Fällen des § 16 Abs. 1 Nr. 2 unterrichtet die übermittelnde Stelle den Betroffenen von der Übermittlung seiner Daten. Dies gilt nicht, wenn damit zu rechnen ist, daß er davon auf andere Weise Kenntnis erlangt, oder wenn die Unterrichtung die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde.** **(5) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.** **(6) Die Stelle, an die die Daten übermittelt werden, ist darauf hinzuweisen, daß die übermittelten Daten nur zu dem Zweck verarbeitet oder genutzt werden dürfen, zu dessen Erfüllung sie übermittelt werden.**	***Begründung (Forts.)*** *Ferner bestimmt die Vorschrift entsprechend Artikel 25 Abs. 1 der Richtlinie, daß im Fall einzelstaatlicher Bestimmungen zur Regelung der Übermittlung personenbezogener Daten in Drittländer, die mit der Richtlinie vereinbar sind, die Vorschriften der §§ 16 Abs. 1 und 28 bis 30 nach Maßgabe dieser Gesetze anzuwenden sind. Entsprechendes 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.* *Absatz 3 beinhaltet dem Artikel 25 Abs. 2 der Richtlinie entnommene Kriterien zur Bestimmung des angemessenen Datenschutzniveaus.* *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.* *Absatz 5 entspricht § 17 Abs. 3 a.F. und Absatz 6 entspricht § 17 Abs. 4 a.F.*

	§ 4 c **Ausnahmen** **(1) Innerhalb des Anwendungsbereichs der in § 4 b Abs. 1 genannten Richtlinie ist eine Übermittlung personenbezogener Daten in ein Drittland oder an eine über- oder zwischenstaatliche Stelle, die kein angemessenes Datenschutzniveau gewährleisten, zulässig, sofern** **1. der Betroffene seine Einwilligung gegeben hat,** **2. die Übermittlung für die Erfüllung eines Vertrags zwischen dem Betroffenen und der verantwortlichen Stelle oder zur Durchführung von vorvertraglichen Maßnahmen, die auf Veranlassung des Betroffenen getroffen worden sind, erforderlich ist,** **3. die Übermittlung zum Abschluß oder zur Erfüllung eines Vertrags erforderlich ist, der im Interesse des Betroffenen von der verantwortlichen Stelle mit einem Dritten geschlossen wurde oder geschlossen werden soll,** **4. die Übermittlung für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist,** **5. die Übermittlung für die Wahrung lebenswichtiger Interessen des Betroffenen erforderlich ist oder**	***Begründung:*** *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.* *Die Regelung des Absatzes 1 ergänzt die strikte Regelung des § 4 b Abs. 2 durch einen weitreichenden Ausnahmekatalog. Diese in Anlehnung an Artikel 26 der Richtlinie formulierten Ausnahmen sollen dafür Sorge tragen, daß der Wirtschaftsverkehr mit Drittländern 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 ein Drittland informiert 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.E. (vgl. auch die Begründung zu § 4 b Abs. 1). Ferner soll der Schutz des Persönlichkeitsrechts zurücktreten, wenn ein wichtiges öffentliches Interesse, die Verteidigung von Rechtsansprüchen vor Gericht oder der für öffentliche Register geltende Publizitätsgrundsatz es erfordern. Hier, wie auch im Fall der Unfähigkeit des Betroffenen seinen Willen zu bekunden (vgl. Nummer 5), ist Maßstab für die Frage der Zulässigkeit und des Umfangs der Übermittlung der Grundsatz der Verhältnismäßigkeit, der eine*

	6. die Übermittlung aus einem Register erfolgt, das zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, soweit die gesetzlichen Voraussetzungen im Einzelfall gegeben sind. **Die Stelle, an die die Daten übermittelt werden, ist darauf hinzuweisen, daß die übermittelten Daten nur zu dem Zweck verarbeitet oder genutzt werden dürfen, zu dessen Erfüllung sie übermittelt werden.** **(2) Unbeschadet des Absatzes 1 kann die zuständige Aufsichtsbehörde eine Übermittlung oder eine Kategorie von Übermittlungen personenbezogener Daten in Drittländer oder an über- oder zwischenstaatliche Stellen genehmigen, die kein angemessenes Schutzniveau im Sinne des § 4 b Abs. 3 gewährleisten, wenn die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist; diese Garantien können sich insbesondere aus Vertragsklauseln <u>oder verbindlichen Unternehmensregelungen</u> ergeben. Bei den in der Telekommunikation oder im Postwesen tätigen Stellen ist der Bundesbeauftragte für den Datenschutz zuständig. Sofern die Übermittlung durch öffentliche Stellen erfolgen soll, nehmen diese die Prüfung nach Satz 1 vor.**	***Begründung (Forts.):*** *Abwägung der widerstreitenden Interessen gebietet. Die Regelung des Absatzes 1 gilt entsprechend dem Grundsatz von § 1 Abs. 4 nicht, wenn einer Übermittlung personenbezogener Daten spezielle Verwendungsbeschränkungen entgegenstehen. In diesem Fall kann trotz Vorliegens der Voraussetzungen des Absatzes 1 von einer Übermittlung in das Drittland abgesehen werden. Dieser Gedanke findet seinen Niederschlag in Artikel 26 Abs. 1 der Richtlinie und in Nummer 60 der Erwägungsgründe. Satz 2 entspricht § 17 Abs. 4 a.F.* *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 Drittland nicht vorhanden ist, kann sie <u>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 Datenschutzniveau angesiedelt sind. Das Verhältnis der Teilunternehmen untereinander ist nicht zwingend durch Vertragsklauseln geprägt. Internationale Konzerne gehen vielmehr vermehrt dazu über, für alle Teilunternehmen unabhängig von ihrem Standort verbindliche Regelungen über den Datenschutz zu erlassen („codes of conduct„). Sowohl Vertragsklauseln als auch verbindliche Unternehmensregelungen</u> sind der Aufsichtsbehörde zur Genehmigung vorzulegen. Im öffentlichen Bereich stellen die verantwortlichen Stellen selbst das Vorliegen ausreichender Garantien im Sinne des Satzes 1 sicher.*

	(3) Die Länder teilen dem Bund ___ die nach Absatz 2 Satz 1 ergangenen Entscheidungen mit.	***Begründung (Forts.):*** *Absatz 3 setzt ___ Artikel 26 Abs. 3 der Richtlinie um. Die in der Richtlinie darüber hinaus vorgesehene Unterrichtungsverpflichtung der Mitgliedstaaten gegenüber der Kommission sowie untereinander bedurfte keiner Umsetzung in nationales Recht.*

	§ 4 d n.F. **Meldepflicht** **(1) Automatisierte Verarbeitungen sind vor ihrer Inbetriebnahme von nicht-öffentlichen verantwortlichen Stellen der zuständigen Aufsichtsbehörde und von öffentlichen verantwortlichen Stellen des Bundes sowie von den in der Telekommunikation oder im Postwesen tätigen Unternehmen dem Bundesbeauftragten für den Datenschutz zu melden.** **(2) Die Meldepflicht entfällt, wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz nach § 4 f bestellt hat. Dies gilt auch, wenn ein Beauftragter bestellt worden ist, ohne daß eine gesetzliche Pflicht zur Bestellung besteht.** **(3) Die Meldepflicht entfällt ferner, wenn die verantwortliche Stelle personenbezogene Daten für eigene Zwecke erhebt, verarbeitet oder nutzt, <u>hierbei höchstens vier Arbeitnehmer mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt und entweder eine Einwilligung der Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit den Betroffenen dient.</u>**	***Begründung:*** *§ 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.* *Die Absätze 2 und 3 beinhalten Ausnahmen von der Meldepflicht.* *Absatz 2 Satz 1 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 Datenschutzbeauftragten 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). Absatz 2 Satz 2 stellt klar, daß die Meldepflicht auch dann entfällt, wenn unbeschadet einer Verpflichtung zur Bestellung eines Datenschutzbeauftragten dieser freiwillig bestellt wird.* *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 Personen, die Empfänger oder Kategorien der Empfänger, denen die Daten weitergegeben werden und die Dauer der Aufbewahrung festgelegt werden. Da die Bestellung eines Datenschutzbeauftragten nach § 4 f Abs. 1 Satz 1 im öffentlichen Bereich obligatorisch ist, die Meldepflicht im öffentlichen Bereich somit bereits nach Absatz 2 entfällt, 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*

.	**§ 4 d n.F. (Forts.)** **(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 Zwecke der Übermittlung oder** **2. zum Zwecke der anonymisierten Übermittlung** **gespeichert werden.** **(5) Soweit ___ automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, unterliegen sie der Prüfung vor Beginn der Verarbeitung (Vorabkontrolle). Eine Vorabkontrolle ist regelmäßig durchzuführen, wenn besondere Arten personenbezogener Daten nach § 3 Abs. 9 verarbeitet werden oder die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit der betroffenen Person zu bewerten einschließlich ihrer Kompetenz, ihrer Leistung oder ihres Verhaltens, es sei denn, dass eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient.** **(6) Zuständig für die Vorabkontrolle ist der Datenschutzbeauftragte nach § 4 f. Dieser nimmt die Vorabkontrolle nach Empfang der Übersicht nach § 4 g Abs. 2 Satz 1 vor. Er hat sich in Zweifelsfällen an die Aufsichtsbehörde oder bei den in der Telekommunikation oder im Postwesen tätigen Unternehmen an den Bundesbeauftragten für den Datenschutz zu wenden.** **___**	***Begründung (Fort.):*** *Reihe von selbständig Berufstätigen, etwa Architekten, Ärzten, Apothekern, Handwerkern, Sanitätshäusern, Optikern, Fitnesstudios 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.* *___* *Absatz 4 ist die Rückausnahme der Absätze 2 und 3. Absatz 4 findet ausweislich seines Wortlauts ("geschäftsmäßig") nur im nichtöffentlichen Bereich Anwendung, die Nummern 1 und 2 entsprechen § 32 Abs. 1 Nr. 1 und 2 a.F.* *Absatz 5 bestimmt in Umsetzung von Artikel 20 Abs. 1 der Richtlinie die automatisierten Verarbeitungen, die der Vorabkontrolle unterliegen. Erwägungsgrund 53 der Richtlinie führt hierzu aus: „Bestimmte Verarbeitungen können jedoch aufgrund ihrer Art, ihrer Tragweite oder ihrer Zweckbestimmung - wie beispielsweise derjenigen, betroffene Personen von der Inanspruchnahme eines Rechts, einer Leistung oder eines Vertrags auszuschließen – oder aufgrund der besonderen Verwendung einer neuen Technologie besondere Risiken im Hinblick auf die Rechte und Freiheiten der betroffenen Personen aufweisen.„ 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. ___*

		Begründung (Forts.): *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 Parlaments 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 einschließlich ihrer Kompetenz, ihrer Leistung oder ihres Verhaltens, als Fälle aufgeführt, in denen eine Vorabkontrolle regelmäßig durchzuführen ist. Um eine sachgerechte Eingrenzung der Fälle der Vorabkontrolle zu erreichen, gilt dies nicht, wenn der Datenverarbeitung eine gesetzliche Verpflichtung oder eine Einwilligung zugrunde liegt oder diese der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient.* *Absatz 6 setzt Artikel 20 Abs. 2 der Richtlinie um. Absatz 6 Satz 1 bestimmt für den Regelfall den Datenschutzbeauftragten als zuständig für die Vorabkontrolle. In Satz 3 konnte auf die Nennung des Bundesbeauftragten für den Datenschutz neben der Aufsichtsbehörde verzichtet werden, da eine Vorabkontrolle nur in Betracht kommt, soweit eine Meldepflicht besteht. Diese entfällt aber wegen der nach § 4 f Abs. 1 obligatorischen Bestellung eines Datenschutzbeauftragten nach § 4 d Abs. 2 Satz 1 im öffentlichen Bereich. Die Regelung der Verfahrensweise des Datenschutzbeauftragten 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 Datenschutzbeauftragten zur Einbindung der Aufsichtsbehörde. In diesem Fall gibt die Aufsichtsbehörde im Rahmen ihrer Befugnisse nach § 38 als Ergebnis ihrer Überprüfung eine Stellungnahme ab.* *___*

	§ 4 e n.F. **Inhalt der Meldepflicht** **Sofern automatisierte Verarbeitungen meldepflichtig sind, sind folgende Angaben zu machen:** **1. Name oder Firma der verantwortlichen Stelle,** **2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,** **3. Anschrift der verantwortlichen Stelle,** **4. Zweckbestimmungen der Datenerhebung, -verarbeitung oder –nutzung,** **5. eine Beschreibung der Kategorien der betroffenen Personen und der diesbezüglichen Daten oder Datenkategorien,** **6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,** **7. Regelfristen für die Löschung der Daten,** **8. eine geplante Datenübermittlung in Drittländer,** **9. eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.** **§ 4 d Abs. 1 und 4 gilt für die Änderung der nach Satz 1 mitgeteilten Angaben sowie für den Zeitpunkt der Aufnahme und der Beendigung der meldepflichtigen Tätigkeit entsprechend.**	***Begründung:*** *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.* *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.* *Nummer 5 setzt Artikel 19 Abs. 1 Buchstabe c der Richtlinie um und entspricht in seinem ersten Teil § 18 Abs. 2 Nr. 4 a.F. Dabei soll insbesondere ersichtlich sein, ob es sich um Daten nach § 3 Abs. 9 handelt.* *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.* *Nummer 7 entspricht § 18 Abs. 2 Nr. 6 a.F.* *Durch Nummer 8 wird Artikel 19 Abs. 1 Buchstabe e der Richtlinie umgesetzt.* *Nummer 9 verwirklicht die Voraussetzungen von Artikel 19 Abs. 1 Buchstabe f der Richtlinie.* *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. **Datenschutzbeauftragter** **(1) Öffentliche und nicht-öffentliche Stellen, die personenbezogene Daten automatisiert erheben, verarbeiten oder nutzen, haben einen Beauftragten für den Datenschutz schriftlich zu bestellen. Nicht-öffentliche Stellen sind hierzu spätestens innerhalb eines Monats nach Aufnahme ihrer Tätigkeit verpflichtet. Das gleiche gilt, wenn personenbezogene Daten auf andere Weise erhoben, verarbeitet oder genutzt werden und damit in der Regel mindestens zwanzig Personen beschäftigt sind. Die Sätze 1 und 2 gelten nicht für nicht-öffentliche Stellen, die höchstens vier Arbeitnehmer mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigen. Soweit aufgrund der Struktur einer öffentlichen Stelle erforderlich, genügt die Bestellung eines Datenschutzbeauftragten für mehrere Bereiche. Soweit nicht-öffentliche Stellen eine Vorabkontrolle durchzuführen haben 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 Datenschutzbeauftragten zu bestellen.** **(2) Zum Beauftragten für den Datenschutz darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Mit dieser Aufgabe kann auch eine Person außerhalb der verantwortlichen Stelle betraut werden. Öffentliche Stellen können mit Zustimmung ihrer Aufsichtsbehörde einen Bediensteten aus einer anderen öffentlichen Stelle zum Beauftragten für den Datenschutz bestellen.**	***Begründung:*** *Die Regelungen des § 4 f gelten sowohl für die betrieblichen als auch für die behördlichen Datenschutzbeauftragten.* *Absatz 1 Satz 1 führt den behördlichen Datenschutzbeauftragten 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 Datenschutzbeauftragten bei automatisierten Datenverarbeitungen in Anlehnung an § 36 Abs. 1 Satz 1 a.F. Die in Satz 5 vorgesehene bereichsübergreifende Bestellung eines Datenschutzbeauftragten 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 Datenschutzbeauftragten 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 wahrgenommen. Diese Organisationsform bleibt durch die zu bestellenden Datenschutzbeauftragten unberührt. Sie werden entsprechend Satz 5 für mehrere Bereiche bestellt und sind auf Zusammenarbeit mit den Aufgabenträgern der Regelorganisation angewiesen. Nur so kann der unvermeidliche zusätzliche Personalaufwand in Grenzen gehalten 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 vorgenannten Stellen verbunden sind. Aus den gleichen Gründen ist es sachgerecht, für Stellen, die regelmäßig eine Vielzahl personenbezogener Daten zum Zwecke der Übermittlung oder der anonymisierten Übermittlung erheben und speichern, unabhängig von der Anzahl der Mitarbeiter eine Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten vorzusehen.* *Absatz 2 Satz 1 entspricht § 36 Abs. 2 a.F. Satz 2 sieht die Möglichkeit vor, sich anstelle eines internen Datenschutzbeauftragten der Dienste eines externen Datenschutzbeauftragten 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 unterstellen. [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 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. **(4) Der Beauftragte für den Datenschutz ist zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit er nicht davon durch den Betroffenen befreit wird.** **(5) Die öffentlichen und nicht-öffentlichen Stellen haben den Beauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen und ihm insbesondere, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist, Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen. Betroffene können sich jederzeit an den Datenschutzbeauftragten wenden.**	***Begründung (Forts.):*** *Absatz 3 entspricht § 36 Abs. 3 a.F., gilt nun aber auch für den behördlichen Datenschutzbeauftragten. 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 ebensowenig entgegen wie der Wahrnehmung 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.* *Absatz 4 entspricht § 36 Abs. 4 a.F.* *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 Datenschutzbeauftragten, vergleichbar der Anrufung des Bundesbeauftragten für den Datenschutz nach § 21.*

	§ 4 g n.F. **Aufgaben des Datenschutzbeauftragten** **(1) Der Beauftragte für den Datenschutz hat die Aufgabe, auf die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz hinzuwirken. Zu diesem Zweck kann sich in Zweifelsfällen der Datenschutzbeauftragte einer öffentlichen Stelle im Benehmen mit dem Leiter der verantwortlichen Stelle an den Bundesbeauftragten für den Datenschutz wenden. Bei Unstimmigkeiten zwischen dem behördlichen Datenschutzbeauftragten und dem Leiter der verantwortlichen Stelle entscheidet die oberste Bundesbehörde, ob sich der behördliche Datenschutzbeauftragte an den Bundesbeauftragten für den Datenschutz wenden darf. Der Datenschutzbeauftragte einer nicht-öffentlichen Stelle kann sich in Zweifelsfällen an die Aufsichtsbehörde oder bei den in der Telekommunikation oder im Postwesen tätigen Unternehmen an den Bundesbeauftragten für den Datenschutz wenden. Er hat insbesondere** **1. die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen; zu diesem Zweck ist er über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten,** **2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderen Vorschriften über den Datenschutz und mit den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut zu machen.** **(2) Dem Beauftragten für den Datenschutz ist von der verantwortlichen Stelle eine Übersicht über die in § 4 e Nr. 1 bis 9 genannten Angaben sowie über zugriffsberechtigte Personen zur Verfügung zu stellen. Im Fall des § 4 d Abs. 2 macht der Beauftragte die Angaben nach Satz 1 mit Ausnahme der Angabe über zugriffsberechtigte Personen sowie der Angaben nach § 4 e Nr. 9 auf Antrag jedermann in geeigneter Weise verfügbar. Im Fall des § 4 d Abs. 3 gilt Satz 2 entsprechend für die verantwortliche Stelle. Satz 2 findet keine Anwendung auf die in § 6 Abs. 2 Satz 4 genannten Behörden.**	***Begründung:*** *Absatz 1 entspricht im wesentlichen § 37 Abs. 1 a.F. Der Begriff „hinzuwirken„ wird der Aufgabe der betrieblichen und auch behördlichen Datenschutzbeauftragten am Besten gerecht. Satz 2 bezieht als Konsequenz des obligatorischen behördlichen Datenschutzbeauftragten den Bundesbeauftragten für den Datenschutz in die Regelung ein, setzt aber insoweit das Benehmen mit dem Leiter der veranwortlichen Stelle voraus. Satz 3 beinhaltet eine Regelung zur Beilegung von Unstimmigkeiten zwischen dem behördlichen Datenschutzbeauftragten und dem Leiter der verantwortlichen Stelle. Satz 4 Nr. 2 enthält eine sprachliche Straffung ohne inhaltliche Auswirkung. 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 Datenschutzbeauftragter vorhanden 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 Datenschutzbeauftragten bestellt hat und auch nicht meldepflichtig nach § 4 d Abs. 3 ist. Die Verpflichtung des Datenschutzbeauftragten, die Angaben auf Antrag jedermann in geeigneter Weise verfügbar zu machen, ist bei den in § 6 Abs. 2 Satz 4 genannten Behörden nicht sachgerecht. Die Anwendbarkeit dieser Vorschrift war daher insoweit auszuschließen.*

§ 5 a. F.	§ 5 n.F.	***Begründung:***
Datengeheimnis Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.	Datengeheimnis Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt **zu erheben**, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.	*In Satz 1 wurde das Wort „erheben„ 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 (vgl. hierzu auch die Begründung zu § 4 Abs. 1).*

§ 6 a. F.	§ 6 n.F.	
Unabdingbare Rechte des Betroffenen	Unabdingbare Rechte des Betroffenen	***Begründung:***
(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.	*Die Änderungen in Absatz 2 sind Folgeänderungen im Zusammenhang mit den Änderungen des Dateibegriffs (vgl. hierzu die Begründung zu § 3 Abs. 2) sowie dem Ersatz des Begriffs der speichernden Stelle durch den der verantwortlichen Stelle (vgl. hierzu die Begründung zu § 3 Abs. 7).*
(2) [1]Sind die Daten des Betroffenen in einer 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 weiterzuleiten. [3]Der Betroffene ist über die Weiterleitung und die speichernde Stelle zu unterrichten. [4]Die in § 19 Abs. 3 genannten Stellen, die Behörden der Staatsanwaltschaft und der Polizei sowie öffentliche Stellen der Finanzverwaltung, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, können statt des Betroffenen den Bundesbeauftragten für den Datenschutz unterrichten. [5]In diesem Fall richtet sich das weitere Verfahren nach § 19 Abs. 6.	(2) Sind die Daten des Betroffenen **automatisiert in der Weise** gespeichert, **daß** mehrere Stellen speicherungsberechtigt sind, und ist der Betroffene nicht in der Lage festzustellen, **welche Stelle die Daten gespeichert hat**, so kann er sich an jede dieser Stellen wenden. Diese ist verpflichtet, das Vorbringen des Betroffenen an die **Stelle, die die Daten gespeichert hat**, weiterzuleiten. Der Betroffene ist über die Weiterleitung und **jene** Stelle zu unterrichten. Die in § 19 Abs. 3 genannten Stellen, die Behörden der Staatsanwaltschaft und der Polizei sowie öffentliche Stellen der Finanzverwaltung, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, können statt des Betroffenen den Bundesbeauftragten für den Datenschutz unterrichten. In diesem Fall richtet sich das weitere Verfahren nach § 19 Abs. 6.	

	§ 6 a 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 automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen.**	***Begründung:*** *§ 6 a setzt Artikel 15 der Richtlinie um. Mit dieser Vorschrift soll verhindert werden, daß Entscheidungen aufgrund von Persönlichkeitsprofilen ergehen, ohne daß der Betroffene die Möglichkeit hat, die zugrundeliegenden Angaben und Bewertungsmaßstäbe zu erfahren. Der Anwendungsbereich der Vorschrift ist dadurch eingeengt, daß es sich um eine Entscheidung handeln muß, die rechtliche Folgen nach sich zieht oder zumindest eine erheblich beeinträchtigende Wirkung hat. Vor allem aber muß die Entscheidung ausschließlich aufgrund einer automatisierten Verarbeitung erfolgen, d.h. eine erneute Überprüfung 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 Verbot durch einzelstaatliches Gesetz, das geeignete Garantien vorsieht, abgesehen werden.* *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 Punktwertverfahren genannt, stellen eine Auswertungsmethode dar, eine Mehrzahl von Menschen oder Merkmalen in eine Reihenfolge nach einem oder mehreren Kriterien zu bringen, d.h. sie zu positionieren. Allerdings fallen Scoring-Verfahren nur dann unter die Regelung, wenn sowohl das Scoring-Verfahren als auch die anschließende Entscheidung in einer Hand liegen. 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 automatisierte Vorauswahl im Vorfeld einer Personalbesetzung (automatisierter Abgleich des Personalbestandes anhand bestimmter Suchkriterien, wie etwa Alter, Ausbildung, Zusatzqualifikation u. ä.), sind nicht erfaßt.* *Identifikationsverfahren, etwa mittels Finger- oder Handabdrücken, der Iris oder der Stimme, werden von der Regelung ebenfalls nicht erfaßt.*

	§ 6 a n.F. (Forts.) **(2) Dies gilt nicht, wenn** **1. die Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertragsverhältnisses oder eines sonstigen Rechtsverhältnisses ergeht und dem Begehren des Betroffenen stattgegeben wurde oder** **2. die Wahrung der berechtigten Interessen des Betroffenen durch geeignete Maßnahmen garantiert und dem Betroffenen von der verantwortlichen Stelle die Tatsache des Vorliegens einer Entscheidung im Sinne des Absatzes 1 mitgeteilt wird. Als geeignete Maßnahme gilt insbesondere die Möglichkeit des Betroffenen, seinen Standpunkt geltend zu machen. Die verantwortliche Stelle ist verpflichtet, ihre Entscheidung erneut zu prüfen.** **(3) Das Recht des Betroffenen auf Auskunft nach § 19 und § 34 erstreckt sich auch auf den logischen Aufbau der automatisierten Verarbeitung der ihn betreffenden Daten.**	***Begründung (Forts.) :*** *Absatz 2 setzt Artikel 15 Abs. 2 Buchstabe a der Richtlinie um und beinhaltet Ausnahmen von Absatz 1.* *Der Begriff des sonstigen Rechtsverhältnisses meint eine der ersten Alternative vergleichbare Fallgestaltung im öffentlichen Bereich.* *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.* *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 Richtlinie deutlich. Der Anwendungsbereich dieses gegenüber dem bisherigen Recht erweiterten Auskunftsrechts beschränkt sich auf die Fälle des § 6 a. Diese Einschränkung wird durch die zugrundeliegende Vorschrift der Richtlinie ermöglicht.*

	§ 6 b 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 dies zur Aufgabenerfüllung, zur Wahrnehmung des Hausrechts oder zur Erfüllung eigener Geschäftszwecke erforderlich ist und keine Anhaltspunkte bestehen, daß schutzwürdige Interessen der betroffenen Personen überwiegen.** **(2) Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen.** **(3) Die Speicherung von nach Absatz 1 erhobenen Daten ist zulässig, wenn dies zum Erreichen des verfolgten Zweckes erforderlich ist.** **(4) 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.**	***Begründung:*** *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 Selbstbestimmungsrechts durch einen angemessenen Interessensausgleich Rechnung trägt. Da bereits die Beobachtung selbst erfaßt wird, kommt es nicht auf das Erfordernis einer anschließenden Speicherung des Bildmaterials an, um datenschutzrechtlich relevant zu sein.* *Die Vorschrift erfaßt nur öffentlich zugängliche Räume wie etwa Bahnsteige, Ausstellungsräume eines Museums, Verkaufsräume oder Schalterhallen. Für nicht öffentlich 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.* *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.* *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.*

	<§ 6 c entfällt> —	—

§ 7 a.F. Schadensersatz durch öffentliche Stellen	**§ 7 n.F. Schadensersatz ___**	***Begründung :***
(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. (2) Bei einer schweren Verletzung des Persönlichkeitsrechts ist dem Betroffenen der Schaden, der nicht Vermögensschaden ist, angemessen in Geld zu ersetzen. (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 Betroffenen 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 verantwortlich ist, bleiben unberührt. (8) Der Rechtsweg vor den ordentlichen Gerichten steht offen.	**(1) Fügt eine verantwortliche Stelle dem Betroffenen durch eine nach den Vorschriften dieses Gesetzes oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten schuldhaft einen Schaden zu, ist ihr Träger dem Betroffenen zum Ersatz dieses Schadens verpflichtet. Die Ersatzpflicht entfällt, soweit die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.** **(2) Mehrere Ersatzpflichtige haften als Gesamtschuldner.** **(3) Vorschriften, nach denen ein Ersatzpflichtiger in weiterem Umfang als nach dieser Vorschrift haftet oder nach denen ein anderer für den Schaden verantwortlich ist, bleiben unberührt.** **(4) Der Rechtsweg vor den ordentlichen Gerichten steht offen.**	*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.* *Absatz 2 entspricht Absatz 5 a.F., Absatz 3 entspricht Absatz 7 a.F. und Absatz 4 entspricht Absatz 8 a.F.*

§ 8 Schadensersatz durch nicht-öffentliche Stellen Macht ein Betroffener gegenüber einer nicht-öffentlichen Stelle einen Anspruch auf Schadensersatz wegen einer nach diesem Gesetz oder anderen Vorschriften über den Datenschutz unzulässigen oder unrichtigen automatisierten Datenverarbeitung geltend und ist streitig, ob der Schaden die Folge eines von der speichernden Stelle zu vertretenden Umstandes ist, so trifft die Beweislast die speichernde Stelle.	**§ 8 n.F.** **Schadensersatz bei automatisierter Datenverarbeitung durch öffentliche Stellen** **(1) Fügt eine verantwortliche öffentliche Stelle dem Betroffenen durch eine nach den Vorschriften dieses Gesetzes oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige automatisierte Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist ihr Träger dem Betroffenen unabhängig von einem Verschulden zum Ersatz des daraus entstehenden Schadens verpflichtet.** **(2) Bei einer schweren Verletzung des Persönlichkeitsrechts ist dem Betroffenen der Schaden, der nicht Vermögensschaden ist, angemessen in Geld zu ersetzen.** **(3) Die Ansprüche nach den Absätzen 1 und 2 sind insgesamt bis zu einem Betrag in Höhe von zweihundertfünfzigtausend Deutsche Mark begrenzt. 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 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.** **(6) § 7 Abs. 2 bis 4 findet entsprechende Anwendung.**	***Begründung:*** *§ 8 entspricht im Wesentlichen § 7 a.F.*

§ 9 a.F. Technische und organisatorische Maßnahmen	§ 9 n.F. Technische und organisatorische Maßnahmen	***Begründung:***
Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.	Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten **erheben,** verarbeiten **oder nutzen,** haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.	*Da Artikel 2 Buchstabe b der Richtlinie auch die Erhebung und Nutzung in den Verarbeitungsbegriff einbezieht, war die Vorschrift entsprechend zu ergänzen.*

	§ 9 a n.F. **Datenschutzaudit** **Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und –programmen ___ ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt.**	***Begründung:*** *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-Staatsvertrag.* *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 Bewertung sowie die Auswahl und Zulassung der Gutachter berufsbeschränkenden Charakter hat und damit dem verfassungsrechtlichen Vorbehalt des Gesetzes unterliegt.*

§ 10 a.F. Einrichtung automatisierter Abrufverfahren	§ 10 n.F. Einrichtung automatisierter Abrufverfahren	***Begründung:***
(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) Die Einrichtung eines automatisierten Verfahrens, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, ist zulässig, soweit dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben oder Geschäftszwecke der beteiligten Stellen angemessen ist. Die Vorschriften über die Zulässigkeit des einzelnen Abrufs bleiben unberührt.	*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.*
(2) Die beteiligten Stellen haben zu gewährleisten, daß die Zulässigkeit des Abrufverfahrens kontrolliert werden kann. Hierzu haben sie schriftlich festzulegen: 1. Anlaß und Zweck des Abrufverfahrens, 2. Datenempfänger, 3. Art der zu übermittelnden Daten, 4. nach § 9 erforderliche technische und organisatorische Maßnahmen. Im öffentlichen Bereich können die erforderlichen Festlegungen auch durch die Fachaufsichtsbehörden getroffen werden.	(2) Die beteiligten Stellen haben zu gewährleisten, daß die Zulässigkeit das Abrufverfahrens kontrolliert werden kann. Hierzu haben sie schriftlich festzulegen: 1. Anlaß und Zweck des Abrufverfahrens, 2. **Dritte, an die übermittelt wird,** 3. Art der zu übermittelnden Daten, 4. nach § 9 erforderliche technische und organisatorische Maßnahmen. Im öffentlichen Bereich können die erforderlichen Festlegungen auch durch die Fachaufsichtsbehörden getroffen werden.	*Entsprechendes gilt für die Neuformulierung von Absatz 4.*
(3) Über die Einrichtung von Abrufverfahren ist in Fällen, in denen die in § 12 Abs. 1 genannten Stellen beteiligt sind, der Bundesbeauftragte für den Datenschutz unter Mitteilung der Festlegungen nach Absatz 2 zu unterrichten. Die Einrichtung von Abrufverfahren, bei denen die in § 6 Abs. 2 und in § 19 Abs. 3 genannten Stellen beteiligt sind, ist nur zulässig, wenn der für die speichernde und die abrufende Stelle jeweils zuständige Bundes- oder Landesminister oder deren Vertreter zugestimmt haben.	(3) Über die Einrichtung von Abrufverfahren ist in Fällen, in denen die in § 12 Abs. 1 genannten Stellen beteiligt sind, der Bundesbeauftragte für den Datenschutz unter Mitteilung der Festlegungen nach Absatz 2 zu unterrichten. Die Einrichtung von Abrufverfahren, bei denen die in § 6 Abs. 2 und in § 19 Abs. 3 genannten Stellen beteiligt sind, ist nur zulässig, wenn **das** für die speichernde und die abrufende Stelle jeweils zuständige Bundes- oder Landesminister**ium** zugestimmt haben.	*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) 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 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.	

(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 aus Datenbeständen, die jedermann, sei es ohne oder nach besonderer Zulassung, zur Benutzung offenstehen.	

§ 11 a.F.	§ 11 n.F.	***Begründung:***
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.*
(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) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei die **Datenerhebung, -verarbeitung** oder –nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind. Er kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden. **Der Auftraggeber hat die Pflicht, sich von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen beim Auftragnehmer zu überzeugen.**	*Absatz 2 Satz 4 setzt Artikel 17 Abs. 2 zweiter Halbsatz der Richtlinie um.*
(3) **1**Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers 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.	(3) Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers **erheben,** verarbeiten oder nutzen. Ist er der Ansicht, daß eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.	*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.*
(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 Datenschutzkontrolle oder die Aufsicht, und zwar für 1. a) öffentliche Stellen, b) nicht-öffentliche Stellen, bei denen der öffentlichen Hand die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht und der Auftraggeber eine öffentliche Stelle ist, die §§ 18, 24 bis 26 oder die entsprechenden Vorschriften der Datenschutzgesetze der Länder, 2. die übrigen nicht-öffentlichen Stellen, soweit sie personenbezogene Daten im Auftrag als Dienstleistungsunternehmen geschäftsmäßig verarbeiten oder nutzen, die §§ 32, 36 bis 38.	(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 Datenschutzkontrolle oder die Aufsicht, und zwar für 1. a) öffentliche Stellen, b) nicht-öffentliche Stellen, bei denen der öffentlichen Hand die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht und der Auftraggeber eine öffentliche Stelle ist, die **§§** 18**,** 24 bis 26 oder die entsprechenden Vorschriften der Datenschutzgesetze der Länder, 2. die übrigen nicht-öffentlichen Stellen, soweit sie personenbezogene Daten im Auftrag als Dienstleistungsunternehmen geschäftsmäßig **erheben,** verarbeiten oder nutzen, die **§§ 4 f , 4 g und** 38.	*Zu Absatz 5:* *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 verantwortlichen Stelle.*
	(5) Die Absätze 1 bis 4 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.	

Zweiter Abschnitt
Datenverarbeitung der öffentlichen Stellen

Erster Unterabschnitt
Rechtsgrundlagen der Datenverarbeitung

§ 12 a.F.	§ 12 n.F.	***Begründung:***
Anwendungsbereich	Anwendungsbereich	*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) 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 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) Soweit der Datenschutz nicht durch Landesgesetz geregelt ist, gelten die **§§ 12 bis 16, 19 bis 20** auch für die öffentlichen Stellen der Länder, soweit sie 1. Bundesrecht ausführen und nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen oder 2. als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt.	*Durch die Ergänzung in Absatz 4 war sicherzustellen, daß Arbeitnehmerdaten unabhängig von dem verwendeten Speichermedium geschützt sind.*
(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 Rechtsverhältnisse 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 Rechtsverhältnisse **erhoben,** verarbeitet oder genutzt, gelten anstelle der **§§ 13 bis 16, 19 bis 20** der § 28 Abs. 1 und **3** Nr. 1 sowie die §§ 33 bis 35, **auch soweit personenbezogene Daten weder automatisiert verarbeitet noch in nicht-automatisierten Dateien verarbeitet oder genutzt oder dafür erhoben werden.**	

§ 13 a.F.	§ 13 n.F.	***Begründung :***
Datenerhebung	Datenerhebung	
(1) Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stellen erforderlich ist.	(1) Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der **verantwortlichen** Stelle erforderlich ist.	*Zu Absatz 1:* *In Absatz 1 steht der Ersatz des Begriffs „erhebenden Stellen„ durch den der „verantwortlichen Stelle„ im Zusammenhang mit dem Ersatz 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 verwiesen.*
(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 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 der Betroffenen beeinträchtigt werden.	**(2) Das Erheben besonderer Arten personenbezogener Daten nach § 3 Abs. 9 ist nur zulässig, soweit** **1. eine Rechtsvorschrift dies vorsieht oder aus Gründen eines wichtigen öffentlichen Interesses zwingend erfordert,** **2. der Betroffene nach Maßgabe des § 4 a Abs. 3 eingewilligt hat,** **3. dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu geben,** **4. es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,** **5. dies zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist,** **6. dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Wahrung erheblicher Belange des Gemeinwohls zwingend erforderlich ist,** **7. dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen,** **8. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluß der Erhebung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann, oder** **9. dies aus zwingenden Gründen der Verteidigung oder der Erfüllung über- oder zwischenstaatlicher Verpflichtungen einer öffentlichen Stelle des Bundes auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Maßnahmen erforderlich ist.**	*Zu Absatz 2:* *Absatz 2 setzt Artikel 8 der Richtlinie um, der ein generelles Verwendungsverbot mit enumerativen Ausnahmetatbeständen für die in § 3 Abs. 9 bezeichneten Daten vorsieht. Durch die Nummern 1 bis 9 werden die nach der Richtlinie möglichen Ausnahmen im Hinblick auf das Bestimmtheitsgebot konkretisiert. Aufgrund der Subsidiarität des Bundesdatenschutzgesetzes nach § 1 Abs. 3 gelten die Einschränkungen des Absatzes 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 Datenschutzregelungen 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.* *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 solche Daten bezogenen Tatbestandsmerkmal einer bereichspezifischen Norm aus Gründen eines wichtigen öffentlichen Interesses zwingend erforderlich ist.* *Nummern 2, 3 und 4 setzen Artikel 8 Abs. 2 Buchstaben a, c und e der Richtlinie um.* *Die Nummern 5 und 6 beruhen auf einer Umsetzung des Artikel 8 Abs. 4 der Richtlinie. Die Anwendbarkeit der Nummer 6 setzt in Anbetracht der Anforderungen des Artikels 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.* *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.* *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.* *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 erhoben, so ist der Erhebungszweck ihm gegenüber anzugeben. [2]Werden sie beim Betroffenen aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. [3]Auf Verlangen ist er über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären.		
(4) Werden personenbezogene Daten statt beim Betroffenen bei einer nichtöffentlichen Stelle erhoben, so ist die Stelle auf die Rechtsvorschrift, die zur Auskunft verpflichtet, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen.		

§ 14 a.F. Datenspeicherung, -veränderung und -nutzung	§ 14 n.F. Datenspeicherung, -veränderung und –nutzung	***Begründung:***
(1) [1]Das Speichern, Verändern oder Nutzen personenbezogener Daten ist zulässig, wenn es zur Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind. [2]Ist keine Erhebung vorausgegangen, dürfen die Daten nur für die Zwecke geändert oder genutzt werden, für die sie gespeichert worden sind. (2) Das Speichern, Verändern oder Nutzen für andere Zwecke ist nur zulässig, wenn 1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt, 2. der Betroffene eingewilligt hat, 3. offensichtlich ist, daß es im Interesse des Betroffenen liegt, und kein Grund zu der Annahme besteht, daß er in Kenntnis des anderen Zwecks seine Einwilligung verweigern würde, 4. Angaben des Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen, 5. die Daten 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, 6. es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit erforderlich ist, 7. es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuches oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist, 8. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder 9. es zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluß der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.	(1) Das Speichern, Verändern oder Nutzen personenbezogener Daten ist zulässig, wenn es zur Erfüllung der in der Zuständigkeit der **verantwortlichen** Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind. Ist keine Erhebung vorausgegangen, dürfen die Daten nur für die Zwecke geändert oder genutzt werden, für die sie gespeichert worden sind. (2) Das Speichern, Verändern oder Nutzen für andere Zwecke ist nur zulässig, wenn 1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt, 2. der Betroffene eingewilligt hat, 3. offensichtlich ist, daß es im Interesse des Betroffenen liegt, und kein Grund zu der Annahme besteht, daß er in Kenntnis des anderen Zwecks seine Einwilligung verweigern würde, 4. Angaben des Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen, 5. Die Daten 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 Zweckänderung offensichtlich überwiegt, 6. Es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit oder **zur Wahrung erheblicher Belange des Gemeinwohls** erforderlich ist, 7. es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuches oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist, 8. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder 9. es zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluß der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.	*Die Änderungen sind Folgeänderungen im Zusammenhang mit dem Ersatz des Begriffs der speichernden Stelle durch den der verantwortlichen Stelle (vgl. hierzu die Begründung zu § 3 Abs. 7).* *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 nach § 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.*

(3) [1]Eine Verarbeitung oder Nutzung für andere Zwecke liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen für die 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. (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.	(3) Eine Verarbeitung oder Nutzung für andere Zwecke liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen für die **verantwortliche** Stelle dient. Das gilt auch für die Verarbeitung oder Nutzung zu Ausbildungs- und Prüfungszwecken durch die **verantwortliche** Stelle, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen. (4) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden. **(5) Das Speichern, Verändern oder Nutzen von besonderen Arten personenbezogener Daten nach § 3 Abs. 9 für andere Zwecke ist nur zulässig, wenn** **1. die Voraussetzungen vorliegen, die eine Erhebung nach § 13 Abs. 2 Nr. 1 bis 6 oder 9 zulassen würden oder** **2. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das öffentliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluß der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.** **Bei der Abwägung nach Satz 1 Nr. 2 ist im Rahmen des öffentlichen Interesses das wissenschaftliche Interesse an dem Forschungsvorhaben besonders zu berücksichtigen.** **(6) Die Speicherung, Veränderung oder Nutzung von besonderen Arten personenbezogener Daten nach § 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.**	***Begründung (Forts.) :*** *In Absatz 5 bedurfte es auf Grund der Regelung der Erhebung besonderer Arten personenbezogener Daten nach § 3 Abs. 9 in Verbindung mit § 13 Abs. 2 einer Bestimmung zur weiteren zweckändernden Verwendung dieser Daten.* *Zu Nummer 1: 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.* *Zu Nummer 2: 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 vorneherein mit einzubeziehen, so daß insoweit keine Zweckänderungen im Sinne der Nummer 2 vorliegen. Das in Nummer 2 statuierte 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 wissenschhaftlichen Interesse an dem Forschungsvorhaben im Rahmen dieser Abwägung besonderes Gewicht zukommt.* *Zu Absatz 6: 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.	***Begründung:***
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 Zuständigkeit der übermittelnden Stelle oder des Empfängers liegenden Aufgaben erforderlich ist und	1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder **des Dritten, an den die Daten übermittelt werden,** liegenden Aufgaben erforderlich ist und	
2. die Voraussetzungen vorliegen, die eine Nutzung nach § 14 zulassen würden.	2. die Voraussetzungen vorliegen, die eine Nutzung nach § 14 zulassen würden.	
(2) **1**Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. **2**Erfolgt die Übermittlung auf Ersuchen des Empfängers, trägt dieser die Verantwor-tung. **3**In diesem Falle prüft die über-mittelnde Stelle nur, ob das Übermit-tlungsersuchen im Rahmen der Auf-gaben des Empfängers liegt, es sei denn, daß besonderer Anlaß zur Prü-fung der Zulässigkeit der Übermittlung besteht. **4**§ 10 Abs. 4 bleibt unberührt.	(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Ersuchen **des Dritten, an den die Daten übermittelt werden**, trägt dieser die Verantwortung. In diesem Falle prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben **des Dritten, an den die Daten über-mittelt werden,** liegt, es sei denn, daß besonderer Anlaß zur Prüfung der Zulässigkeit der Übermittlung besteht. § 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) **Der Dritte, an den die Daten übermittelt werden, darf diese** für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nur unter den Voraussetzungen des § 14 Abs. 2 zulässig.	*Hinsichtlich des Verzichts auf den Begriff „Akten„ in Absatz 5 wird auf die Begründung zu § 3 Abs. 2 verwiesen.*
(4) Für die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgesellschaf-ten 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 Religionsgesellschaf-ten gelten die Absätze 1 bis 3 entsprechend, sofern sichergestellt ist, daß bei **diesen** ausreichende Datenschutzmaßnahmen getroffen werden.	
(5) Sind mit personenbezogenen Daten, die nach Absatz 1 übermittelt werden dürfen, weitere personenbe-zogene Daten des Betroffenen oder eines Dritten in Akten so verbunden, daß eine Trennung nicht oder nur mit un-vertretbarem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht berech-tigte Interessen des Betroffenen oder eines Dritten an deren Geheimhaltung offen-sichtlich überwiegen; eine Nutzung dieser Daten ist unzulässig.	(5) Sind mit personenbezogenen Daten, die nach Absatz 1 übermittelt werden dürfen, weitere personenbezogene Daten des Betroffenen oder eines Dritten so verbunden, daß eine Trennung nicht oder nur mit un-vertretbarem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht berechtigte Inter-essen des Betroffenen oder eines Drit-ten an deren Geheimhaltung offen-sichtlich überwiegen; 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. Datenübermittlung an nicht-öffentliche Stellen	§ 16 n.F. Datenübermittlung an nicht-öffentliche Stellen	***Begründung:***
(1) Die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen ist zulässig, wenn 1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 14 zulassen würden, oder 2. der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat.	(1) Die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen ist zulässig, wenn 1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 14 zulassen würden, oder 2. **der Dritte, an den die Daten übermittelt werden**, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat. **Das Übermitteln von besonderen Arten personenbezogener Daten nach § 3 Abs. 9 ist <u>abweichend von Satz 1 Nr. 2</u> nur zulässig, (__) soweit dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist.**	*Zur Ersetzung des Begriffs des Empfängers durch den Begriff des Dritten, an den die Daten übermittelt werden, wird auf die Begründung zu § 15 verwiesen.* *Die Ergänzung in Absatz 1 Nr. 2 Satz 2 ___ 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. (3) **1**In den Fällen der Übermittlung nach Absatz 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 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. 3Eine Verarbeitung oder Nutzung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Absatz 1 zulässig wäre und die übermittelnde Stelle zugestimmt hat.	(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 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 Wohle des Bundes oder eines Landes Nachteile bereiten würde. (4) **Der Dritte, an den die Daten übermittelt werden, darf diese** nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Die übermittelnde Stelle hat **ihn** darauf hinzuweisen. Eine Verarbeitung oder Nutzung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Absatz 1 zulässig wäre und die übermittelnde Stelle zugestimmt hat.	

§ 17 a.F. 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. (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 dürfen, zu dessen Erfüllung sie ihm übermittelt werden.	Hinweis: Die Vorschrift wurde vollständig aufgehoben.	***Begründung:*** *Auf die Begründung zu § 4 b wird verwiesen.*

§ 18 a.F. Durchführung des Datenschutzes in der Bundesverwaltung	§ 18 n.F. Durchführung des Datenschutzes in der Bundesverwaltung	***Begründung:***
(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. 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) Die obersten Bundesbehörden, der Präsident des Bundeseisenbahnvermögens, sowie die bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, über die von der Bundesregierung oder einer obersten Bundesbehörde lediglich die Rechtsaufsicht ausgeübt wird, haben für ihren Geschäftsbereich die Ausführung dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen. Das gleiche gilt für die Vorstände der aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange ihnen ein ausschließliches Recht nach dem Postgesetz zusteht.	*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.*
(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. **3**Sie haben ferner dafür zu sorgen, daß die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, überwacht wird.	(2) **1**Die öffentlichen Stellen führen ein Verzeichnis der eingesetzten Datenverarbeitungsanlagen. Für ihre **automatisierten Verarbeitungen** haben sie **die Angaben nach § 4 e sowie die Rechtsgrundlage der Verarbeitung** schriftlich festzulegen. **Bei allgemeinen Verwaltungszwecken dienenden automatisierten Verarbeitungen, bei welchen das Auskunftsrecht des Betroffenen nicht nach § 19 Abs. 3 oder 4 eingeschränkt wird, kann hiervon abgesehen werden. Für automatisierte Verarbeitungen, die in gleicher oder ähnlicher Weise mehrfach geführt werden, können die Festlegungen zusammengefaßt werden.**	*Zu Absatz 2 Satz 3 bis 5: 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.).* *Die umzusetzende Richtlinie sieht eine Privilegierungsmöglichkeit für nur vorübergehend vorgehaltene Dateien im Sinne des § 18 Abs. 3 a.F. nicht vor. Die Vorschrift des Absatzes 3 war daher ersatzlos aufzuheben.*
(3) Absatz 2 Satz 2 gilt nicht für Dateien, die nur vorübergehend vorgehalten und innerhalb von drei Monaten nach ihrer Erstellung gelöscht werden.		

	Zweiter Unterabschnitt **Rechte des Betroffenen**	
§ 19 a.F. Auskunft an den Betroffenen (1) **1**Dem Betroffenen ist auf Antrag Auskunft zu erteilen über 1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf Herkunft oder Empfänger dieser Daten beziehen, und 2. den Zweck der Speicherung. **2**In dem Antrag soll die Art der personenbezo-genen 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 Ertei-lung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffe-nen geltend gemachten Informationsinteresse steht. **4**Die speichernde Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen. (2) Absatz 1 gilt nicht für personenbezogene Daten, die nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen. (3) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundes-ministers der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig. (4) Die Auskunftserteilung unterbleibt, soweit 1. die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben gefährden würde, 2. die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder 3. die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheimgehalten werden müssen und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muß.	§ 19 n.F. Auskunft an den Betroffenen (1) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über 1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen, 2. **die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden,** und 3. den Zweck der Speicherung. **2**In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. **3**Sind die personenbezogenen Daten **weder automatisiert noch in <u>nicht-automatisierten</u> Dateien** gespeichert, wird die Auskunft nur erteilt, soweit der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht. **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 werden dürfen, oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen **und eine Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.** (3) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundes-minister**iums** der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig. (4) Die Auskunftserteilung unterbleibt, soweit 1. die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der **verantwortlichen** Stelle liegenden Aufgaben gefährden würde, 2. die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder 3. die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheimgehalten werden müssen und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muß.	***Begründung:*** *Durch die Neufassung des Absatzes 1 wird Artikel 12 Buchstabe a, 1. Spiegelstrich der Richtlinie umgesetzt.* *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.* *Die Änderungen in Absatz 1 Satz 4, Absatz 4 und 6 sind Folgeänderungen im Zusammenhang mit dem Ersatz des Begriffs der speichernden Stelle durch den der verantwortlichen Stelle (vgl. hierzu die Begründung zu § 3 Abs. 7). Hinsichtlich des Ersatzes des Wortes „Akten„ durch die Wörter „weder automatisiert noch in <u>nicht-automatisierten</u> Dateien„ in Absatz 1 Satz 3 wird auf die Begründung zu § 3 Abs. 2 verwiesen.* *Die Ausnahme des Absatzes 2 Satz 1 wurde in Anwendung des Artikels 13 Abs. 1 Buchstabe g der Richtlinie modifiziert.* *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.*

(5) **1**Die Ablehnung der Auskunftserteilung bedarf einer Begründung nicht, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. **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 zuständige oberste Bundesbehörde im Einzelfall feststellt, daß dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. **2**Die Mitteilung des Bundesbeauftragten an den Betroffenen darf keine Rückschlüsse auf den Er-kenntnisstand der speichernden Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt. (7) Die Auskunft ist unentgeltlich.	(5) Die Ablehnung der Auskunftserteilung bedarf einer Begründung nicht, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Falle ist der Betroffene darauf hinzuweisen, daß er sich an den Bundesbeauftragten für den Datenschutz 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 zuständige oberste Bundesbehörde im Einzelfall feststellt, daß dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. **2**Die Mitteilung des Bundesbeauftragten an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand der **verantwortlichen** Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt. (7) Die Auskunft ist unentgeltlich. .	

	§ 19 a n.F. **Benachrichtigung** **(1) Werden Daten ohne Kenntnis des Betroffenen erhoben, so ist er von der Speicherung, der Identität der verantwortlichen Stelle sowie über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung zu unterrichten. Der Betroffene ist auch über die Empfänger oder Kategorien von Empfängern von Daten zu unterrichten, soweit er nicht mit der Übermittlung an diese rechnen muß. Sofern eine Übermittlung vorgesehen ist, hat die Unterrichtung spätestens bei der ersten Übermittlung zu erfolgen.** **(2) Eine Pflicht zur Benachrichtigung besteht nicht, wenn** **1. der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat,** **2. die Unterrichtung des Betroffenen einen unverhältnismäßigen Aufwand erfordert oder** **3. die Speicherung oder Übermittlung der personenbezogenen Daten durch Gesetz ausdrücklich vorgesehen ist.** **Die verantwortliche Stelle legt schriftlich fest, unter welchen Voraussetzungen von einer Benachrichtigung nach Nummer 2 oder 3 abgesehen wird.** **(3) § 19 Abs. 2 bis 4 gilt entsprechend.**	***Begründung:*** *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.* *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 beruhen auf Artikel 13 der Richtlinie.* *Durch Absatz 2 Satz 2 wird das Erfordernis der „geeigneten Garantien„ nach Artikel 11 Abs. 2 Satz 2 der Richtlinie umgesetzt. Der behördliche Datenschutzbeauftragte wirkt auf die Einhaltung dieser Vorschrift hin.*

§ 20 a.F.	§ 20 n.F.	***Begründung:***
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) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Wird festgestellt, daß personenbezogene Daten, **die weder automatisiert verarbeitet noch in <u>nicht-automatisierten</u> Dateien gespeichert sind**, unrichtig sind, oder wird ihre Richtigkeit von dem Betroffenen bestritten, so ist dies in **geeigneter** Weise festzuhalten.	*Zu Absatz 1:* *Hinsichtlich des Ersatzes des Wortes „Akten„ durch die Wörter „weder automatisiert verarbeitet noch in <u>nicht-automatisierten</u> 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 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.	(2) Personenbezogene Daten, **die automatisiert verarbeitet oder in <u>nicht-automatisierten</u> 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.	*Zu Absatz 2:* *Hinsichtlich der Änderung in Satz 1 vor Nr. 1 wird auf die Begründung zu § 3 Abs. 2 verwiesen. Die Änderung in Absatz 2 Nr. 2 ist eine Folgeänderung im Zusammenhang mit dem Ersatz 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.	*Zu Absatz 4: Auf die Begründung zu § 3 Abs. 2 wird verwiesen.*
(4) Personenbezogene Daten in Dateien sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen läßt.	(4) Personenbezogene Daten, **die automatisiert verarbeitet oder in <u>nicht-automatisierten</u> Dateien gespeichert sind,** sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen läßt.	

	(5) Personenbezogene Daten dürfen nicht für eine automatisierte Verarbeitung oder Verarbeitung in <u>nicht-automatisierten</u> 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. <u>Satz 1 gilt nicht, wenn eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung verpflichtet.</u>	***Begründung (Forts.):***
(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.	(**6**) Personenbezogene Daten, **die weder automatisiert verarbeitet noch in einer <u>nicht-automatisierten</u> Datei gespeichert sind,** sind zu sperren, wenn die Behörde im Einzelfall feststellt, daß ohne die Sperrung schutzwürdige Interessen des Betroffenen beeinträchtigt würden und die Daten für die Aufgabenerfüllung der Behörde nicht mehr erforderlich sind.	*Zu Absatz 5:* *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 Betroffenen 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 Widerspruch 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 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). <u>Wie Art. 14 Buchstabe a in Verbindung mit Art. 7 Buchstabe c der Richtlinie zulässt, schließt Satz 2 das Widerspruchsrecht in den Fällen aus, in denen eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung verpflichtet.</u>* *Nach Artikel 14 Buchstabe a, zweiter Halbsatz der Richtlinie kann das einzelstaatliche Recht einen Ausschluss des Widerspruchsrechts vorsehen.*
(6) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn 1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der 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**) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn 1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der **verantwortlichen** Stelle oder eines Dritten liegenden Gründen unerläßlich ist und 2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.	*Zu Absatz 6:* *Hinsichtlich des Ersatzes des Wortes „Akten„ durch die Wörter „weder automatisiert verarbeitet noch in einer <u>nicht-automatisierten</u> Datei gespeichert„ wird auf die Begründung zu § 3 Abs. 2 verwiesen.* *Zu Absatz 7:* *Die Änderung in Absatz 7 Nr. 1 ist eine Folgeänderung im Zusammenhang mit dem Ersatz des Begriffs der speichernden Stelle durch den der verantwortlichen Stelle (vgl. hierzu die Begründung zu § 3 Abs. 7).*

§ 20 a.F. (Forts.)	§ 20 n.F. (Forts.)	***Begründung (Forts.):***
(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 Daten zur Speicherung weitergegeben werden, wenn dies zur Wahrung schutzwürdiger Interessen des Betroffenen erforderlich ist. (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 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.	*Zu Absatz 8:* *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. 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.*

§ 21 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.	*Hinweis: Vorschrift ist unverändert*	

Dritter Unterabschnitt
Bundesbeauftragter für den Datenschutz

§ 22 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. (2) [1]Der Beauftragte 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." [2]Der Eid kann auch ohne religiöse Beteuerung geleistet werden. (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 Amtsverhältnis. [2]Er ist in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. [3]Er untersteht der Rechtsaufsicht der Bundesregierung. (5) Der Bundesbeauftragte wird beim Bundesminister des Innern eingerichtet. Er untersteht der Dienstaufsicht des Bundesministers des Innern. 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. Die Stellen sind im Einvernehmen mit dem Bundesbeauftragten zu besetzen. Die Mitarbeiter können, falls sie mit der beabsichtigten Maßnahme nicht einverstanden sind, nur im Einvernehmen mit ihm versetzt, abgeordnet oder umgesetzt werden. (6) Ist der Bundesbeauftragte vorübergehend an der Ausübung seines Amtes verhindert, kann der Bundesminister des Innern einen Vertreter mit der Wahrnehmung der Geschäfte beauftragen. Der Bundesbeauftragte soll dazu gehört werden.	§ 22 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. (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." [2]Der Eid kann auch ohne religiöse Beteuerung geleistet werden. (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 Amtsverhältnis. [2]Er ist in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. [3]Er untersteht der Rechtsaufsicht der Bundesregierung. (5) Der Bundesbeauftragte wird beim Bundesminister**ium** des Innern eingerichtet. Er untersteht der Dienstaufsicht des Bundesminister**iums** des Innern. Dem Bundesbeauftragten ist die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen; sie ist im Einzelplan des Bundesminister**iums** des Innern in einem eigenen Kapitel auszuweisen. Die Stellen sind im Einvernehmen mit dem Bundesbeauftragten zu besetzen. Die Mitarbeiter können, falls sie mit der beabsichtigten Maßnahme nicht einverstanden sind, nur im Einvernehmen mit ihm versetzt, abgeordnet oder umgesetzt werden. (6) Ist der Bundesbeauftragte vorübergehend an der Ausübung seines Amtes verhindert, kann der Bundesminister des Innern einen Vertreter mit der Wahrnehmung der Geschäfte beauftragen. Der Bundesbeauftragte soll dazu gehört werden.	***Begründung:*** *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.*	

§ 23 a.F. Rechtsstellung des Bundesbeauftragten für den Datenschutz	§ 23 n.F. Rechtsstellung des Bundesbeauftragten für den Datenschutz	***Begründung:***
(1) Das Amtsverhältnis des Bundesbeauftragten für den Datenschutz beginnt mit der Aushändigung der Ernennungsurkunde. Es endet 1. mit Ablauf der Amtszeit, 2. mit der Entlassung. Der Bundespräsident entläßt den Bundesbeauftragten, wenn dieser es verlangt oder auf Vorschlag der Bundesregierung, wenn Gründe vorliegen, die bei einem Richter auf Lebenszeit die Entlassung aus dem Dienst rechtfertigen. Im Falle der Beendigung des Amtsverhältnisses erhält der Bundesbeauftragte eine vom Bundespräsidenten vollzogene Urkunde. Eine Entlassung wird mit der Aushändigung der Urkunde wirksam. Auf Ersuchen des Bundesministers des Innern ist der Bundesbeauftragte verpflichtet, die Geschäfte bis zur Ernennung seines Nachfolgers weiterzuführen.	(1) Das Amtsverhältnis des Bundesbeauftragten für den Datenschutz beginnt mit der Aushändigung der Ernennungsurkunde. Es endet 1. mit Ablauf der Amtszeit, 2. mit der Entlassung. Der Bundespräsident entläßt den Bundesbeauftragten, wenn dieser es verlangt oder auf Vorschlag der Bundesregierung, wenn Gründe vorliegen, die bei einem Richter auf Lebenszeit die Entlassung aus dem Dienst rechtfertigen. Im Falle der Beendigung des Amtsverhältnisses erhält der Bundesbeauftragte eine vom Bundespräsidenten vollzogene Urkunde. Eine Entlassung wird mit der Aushändigung der Urkunde wirksam. Auf Ersuchen des Bundesministers des Innern ist der Bundesbeauftragte verpflichtet, die Geschäfte bis zur Ernennung seines Nachfolgers weiterzuführen.	*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.*
(2) Der Bundesbeauftragte darf neben seinem Amt kein anderes besoldetes Amt, kein Gewerbe und keinen Beruf ausüben und weder der Leitung oder dem Aufsichtsrat oder Verwaltungsrat eines auf Erwerb gerichteten Unternehmens noch einer Regierung oder einer gesetzgebenden Körperschaft des Bundes oder eines Landes angehören. Er darf nicht gegen Entgelt außergerichtliche Gutachten abgeben.	(2) Der Bundesbeauftragte darf neben seinem Amt kein anderes besoldetes Amt, kein Gewerbe und keinen Beruf ausüben und weder der Leitung oder dem Aufsichtsrat oder Verwaltungsrat eines auf Erwerb gerichteten Unternehmens noch einer Regierung oder einer gesetzgebenden Körperschaft des Bundes oder eines Landes angehören. Er darf nicht gegen Entgelt außergerichtliche Gutachten abgeben.	
(3) Der Bundesbeauftragte hat dem Bundesminister des Innern Mitteilung über Geschenke zu machen, die er in bezug auf sein Amt erhält. Der Bundesminister des Innern entscheidet über die Verwendung der Geschenke.	(3) Der Bundesbeauftragte hat dem Bundesminister**ium** des Innern Mitteilung über Geschenke zu machen, die er in bezug auf sein Amt erhält. Das Bundesminister**ium** des Innern entscheidet über die Verwendung der Geschenke.	
(4) Der Bundesbeauftragte ist berechtigt, über Personen, die ihm in seiner Eigenschaft als Bundesbeauftragter Tatsachen anvertraut haben, sowie über diese Tatsachen selbst das Zeugnis zu verweigern. Dies gilt auch für die Miarbeiter des Bundesbeauftragten mit der Maßgabe, daß über die Ausübung dieses Rechts der Bundesbeauftragte entscheidet. Soweit das Zeugnisverweigerungsrecht des Bundesbeauftragten reicht, darf die Vorlegung oder Auslieferung von Akten oder anderen Schriftstücken von ihm nicht gefordert werden.	(4) Der Bundesbeauftragte ist berechtigt, über Personen, die ihm in seiner Eigenschaft als Bundesbeauftragter Tatsachen anvertraut haben, sowie über diese Tatsachen selbst das Zeugnis zu verweigern. Dies gilt auch für die Mitarbeiter des Bundesbeauftragten mit der Maßgabe, daß über die Ausübung dieses Rechts der Bundesbeauftragte entscheidet. Soweit das Zeugnisverweigerungsrecht des Bundesbeauftragten reicht, darf die Vorlegung oder Auslieferung von Akten oder anderen Schriftstücken von ihm nicht gefordert werden.	

§ 23 a.F. (Forts.)	§ 23 n.F. (Forts.)	***Begründung (Forts.):***
(5) Der Bundesbeauftragte ist, auch nach Beendigung seines Amtsverhältnisses, verpflichtet, über die ihm amtlich bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Der Bundesbeauftragte darf, auch wenn er nicht mehr im Amt ist, über solche Angelegenheiten ohne Genehmigung des Bundesministers des Innern weder vor Gericht noch außer-gerichtlich aussagen oder Erklärungen abgeben. Unberührt bleibt die gesetzlich begründete Pflicht, Straftaten anzuzeigen und bei Gefährdung der freiheitlichen demokratischen Grundordnung für deren Erhaltung einzutreten.	(5) Der Bundesbeauftragte ist, auch nach Beendigung seines Amtsverhältnisses, verpflichtet, über die ihm amtlich bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Der Bundesbeauftragte darf, auch wenn er nicht mehr im Amt ist, über solche Angelegenheiten ohne Genehmigung des Bundesminister**iums** des Innern weder vor Gericht noch außergerichtlich aussagen oder Erklärungen abgeben. Unberührt bleibt die gesetzlich begründete Pflicht, Straftaten anzuzeigen und bei Gefährdung der freiheitlichen demokratischen Grundordnung für deren Erhaltung einzutreten. **Für den Bundesbeauftragten und seine Mitarbeiter gelten die §§ 93, 97, 105 Abs. 1, 111 Abs. 5 in Verbindung mit 105 Abs. 1 sowie 116 Abs. 1 der Abgabenordnung nicht. Satz 5 findet keine Anwendung, soweit die Finanzbehörden die Kenntnis für die Durchführung eines Verfahrens wegen einer Steuerstraftat sowie eines damit zusammenhängenden Steuerverfahrens benötigen, an deren Verfolgung ein zwingendes öffentliches Interesse besteht, oder soweit es sich um vorsätzlich falsche Angaben des Auskunftspflichtigen oder der für ihn tätigen Personen handelt. Stellt der Bundesbeauftragte einen Datenschutzverstoß fest, ist er befugt, diesen anzuzeigen und den Betroffenen hierüber zu informieren.**	*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 Bundesbeauftragten für den Datenschutz sowie dessen Recht, Betroffene zu informieren.*
(6) Die Genehmigung, als Zeuge auszusagen, soll nur versagt werden, wenn die Aussage dem Wohle des Bundes oder eines deutschen Landes Nachteile bereiten oder die Erfüllung öffentlicher Aufgaben ernstlich gefährden oder erheblich erschweren würde. Die Genehmigung, ein Gutachten zu erstatten, kann versagt werden, wenn die Erstattung den dienstlichen Interessen Nachteile bereiten würde. § 28 des Gesetzes über das Bundesverfassungsgericht in der Fassung der Bekanntmachung vom 12. Dezember 1985 (BGBl. I S. 2229) bleibt unberührt.	(6) Die Genehmigung, als Zeuge auszusagen, soll nur versagt werden, wenn die Aussage dem Wohle des Bundes oder eines deutschen Landes Nachteile bereiten oder die Erfüllung öffentlicher Aufgaben ernstlich gefährden oder erheblich erschweren würde. Die Genehmigung, ein Gutachten zu erstatten, kann versagt werden, wenn die Erstattung den dienstlichen Interessen Nachteile bereiten würde. § 28 des Gesetzes über das Bundesverfassungsgericht in der Fassung der Bekanntmachung vom 12. Dezember 1985 (BGBl. I S. 2229) bleibt unberührt.	

§ 23 a.F. (Forts.):	§ 23 n.F. (Forts.):	***Begründung (Forts.):***
(7) Der Bundesbeauftragte erhält vom Beginn des Kalendermonats an, in dem das Amtsverhältnis beginnt, bis zum Schluß des Kalendermonats, in dem das Amtsverhältnis endet, im Falle des Absatzes 1 Satz 6 bis zum Ende des Monats, in dem die Geschäftsführung endet, Amtsbezüge in Höhe der einem Bundesbeamten der Besoldungsgruppe B 9 zustehenden Besoldung. Das Bundesreisekostengesetz und das Bundesumzugskostengesetz sind entsprechend anzuwenden. Im übrigen sind die §§ 13 bis 20 des Bundesministergesetzes in der Fassung der Bekanntmachung vom 27. Juli 1971 (BGBl. I S. 1166), zuletzt geändert durch das Gesetz zur Kürzung des Amtsgehalts der Mitglieder der Bundesregierung und der Parlamentarischen Staatssekretäre vom 22. Dezember 1982 (BGBl. I S. 2007), mit der Maßgabe anzuwenden, daß an die Stelle der zweijährigen Amtszeit in § 15 Abs. 1 des Bundesministergesetzes eine Amtszeit von fünf Jahren tritt. Abweichend von Satz 3 in Verbindung mit den §§ 15 bis 17 des Bundesministergesetzes berechnet sich das Ruhegehalt des Bundesbeauftragten unter Hinzurechnung der Amtszeit als ruhegehaltsfähige Dienstzeit in entsprechender Anwendung des Beamtenversorgungsgesetzes, wenn dies günstiger ist und der Bundesbeauftragte sich un-mittelbar vor seiner Wahl zum Bundesbeauftragten als Beamter oder Richter mindestens in dem letzten gewöhnlich vor Erreichen der Besoldungsgruppe B 9 zu durchlaufenden Amt befunden hat.	(7) Der Bundesbeauftragte erhält vom Beginn des Kalendermonats an, in dem das Amtsverhältnis beginnt, bis zum Schluß des Kalendermonats, in dem das Amtsverhältnis endet, im Falle des Absatzes 1 Satz 6 bis zum Ende des Monats, in dem die Geschäftsführung endet, Amtsbezüge in Höhe der einem Bundesbeamten der Besoldungsgruppe B 9 zustehenden Besoldung. Das Bundesreisekostengesetz und das Bundesumzugskostengesetz sind entsprechend anzuwenden. Im übrigen sind die §§ 13 bis 20 des Bundesministergesetzes in der Fassung der Bekanntmachung vom 27. Juli 1971 (BGBl. I S. 1166), zuletzt geändert durch das Gesetz zur Kürzung des Amtsgehalts der Mitglieder der Bundesregierung und der Parlamentarischen Staatssekretäre vom 22. Dezember 1982 (BGBl. I S. 2007), mit der Maßgabe anzuwenden, daß an die Stelle der zweijährigen Amtszeit in § 15 Abs. 1 des Bundesministergesetzes eine Amtszeit von fünf Jahren tritt. Abweichend von Satz 3 in Verbindung mit den §§ 15 bis 17 des Bundesministergesetzes berechnet sich das Ruhegehalt des Bundesbeauftragten unter Hinzurechnung der Amtszeit als ruhegehaltsfähige Dienstzeit in entsprechender Anwendung des Beamtenversorgungsgesetzes, wenn dies günstiger ist und der Bundesbeauftragte sich unmittelbar vor seiner Wahl zum Bundesbeauftragten als Beamter oder Richter mindestens in dem letzten gewöhnlich vor Erreichen der Besoldungsgruppe B 9 zu durchlaufenden Amt befunden hat. **(8) Absatz 5 Satz 5 bis 7 gilt entsprechend für die öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind.**	*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.*

§ 24 a.F. Kontrolle durch den Bundesbeauftragten für den Datenschutz	§ 24 n.F. Kontrolle durch den Bundesbeauftragten für den Datenschutz	***Begründung:***
(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 Betroffene ihm hinreichende Anhaltspunkte dafür darlegt, daß er dabei in seinen Rechten verletzt worden ist, oder dem Bundesbeauftragten 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.	***Zu Absatz 1:*** *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 Kontrolle durch den Bundesbeauftragten unterliegen nicht: 1. personenbezogene Daten, die der Kontrolle durch die Kommission nach § 9 des Gesetzes zu Artikel 10 Grundgesetz 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) **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.** **2Das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses des Artikels 10 des Grundgesetzes wird insoweit eingeschränkt.** **3Personenbezogene Daten**, die der Kontrolle durch die Kommission nach § 9 des Gesetzes zu Artikel 10 Grundgesetz unterliegen, **unterliegen nicht der Kontrolle durch den Bundesbeauftragten,** es sei denn, die Kommission ersucht den Bundesbeauftragten, die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten. **Der Kontrolle durch den Bundesbeauftragten unterliegen auch nicht** personenbezogene Daten in Akten über die Sicherheitsüberprüfung, wenn der Betroffene der Kontrolle der auf ihn bezogenen Daten im Einzelfall gegenüber dem Bundesbeauftragten widerspricht.	*Zu Absatz 2 Satz 1 und 2:* *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 Neufassung von § 24 Abs. 1 und 2 beseitigt worden. Keine ausdrückliche Regelung enthält das geltende Recht 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 des geltenden Rechts, der den Inhalt des Post- und Fernmeldeverkehrs von der Kontrolle ausnimmt, 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 vorgesehenen 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.*

§ 24 a.F. (Forts.)	§ 24 n.F. (Forts.)	***Begründung (Forts.):***
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 gegenüber 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. (3) Die Bundesgerichte unterliegen der Kontrolle des Bundesbeauftragten nur, soweit sie in Verwaltungsangelegenheiten tätig werden. (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 Einsicht 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, 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 Beauftragten. **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 Nutzung personenbezogener Daten, verbinden. **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.	(3) **Bei den Bundesgerichten ist die unmittelbar der Rechtsprechung dienende Tätigkeit der Richter von der Kontrolle ausgenommen.** (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 Einsicht in alle Unterlagen, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Kontrolle nach Absatz 1 stehen, 2. jederzeit Zutritt in alle Diensträume zu gewähren. **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 Beauftragten. **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 Nutzung personenbezogener Daten, verbinden. **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.	***Zu Absatz 2 Satz 3:*** *Die Neuformulierung des Satzes 3 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, 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. Auch das Widerspruchsrecht in Bezug auf die Kontrolle des Bundesbeauftragten für den Datenschutz in Akten über die Sicherheitsüberprüfung wurde gestrichen.* *Die Neuregelung des Absatzes 3 präzisiert die Ausnahmen von der Kontrolle durch den Bundesbeauftragten für den Datenschutz im Bereich der Justiz.* *Zur Streichung des Begriffs der Akte in Absatz 4 vergleiche die Begründung zu § 3 Abs. 2.*

§ 25 a.F. 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 oder Nutzung personenbezogener Daten fest, so beanstandet er dies 1. bei der Bundesverwaltung gegenüber der zuständigen obersten Bundesbehörde, 2. beim Bundeseisenbahnvermögen gegenüber dem Präsidenten, 3. bei den aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unterneh-men, solange ihnen ein ausschließliches Recht nach dem Postgesetz zusteht, gegenüber deren Vorständen, 4. bei den bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie bei Vereinigungen solcher Körperschaften, Anstalten und Stiftungen gegenüber dem Vorstand oder dem sonst vertretungsberechtigten Organ und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf. [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 Mängel 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 Stellungnahme an den Bundesbeauftragten zu.	*Hinweis:* *Die Vorschrift bleibt unverändert.*	*:*

§ 26 a.F. Weitere Aufgaben des Bundesbeauftragten für den Datenschutz; Dateienregister	§ 26 n.F. Weitere Aufgaben des Bundesbeauftragten für den Datenschutz	***Begründung:***
(1) **1**Der Bundesbeauftragte für den Datenschutz erstattet dem Deutschen Bundestag alle zwei Jahre einen Tätigkeitsbericht. **2**Der Tätigkeitsbericht soll auch eine Darstellung der wesentlichen Entwicklung des Datenschutzes im nicht-öffentlichen Bereich enthalten. (2) **1**Auf Anforderung des Deutschen Bundestages oder der Bundesregierung hat der Bundesbeauftragte Gutachten zu erstellen und Berichte zu erstatten. **2**Auf Ersuchen des Deutschen Bundestages, des Petitionsausschusses, des Innenausschusses oder der Bundesregierung geht der Bundesbeauftragte ferner Hinweisen auf Angelegenheiten und Vorgänge des Datenschutzes bei den öffentlichen Stellen des Bundes nach. **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 Empfehlungen zur Verbesserung des Datenschutzes geben und sie in Fragen des Datenschutzes 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 Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind, sowie mit den Aufsichtsbehörden nach § 38 hin. (5) **1**Der Bundesbeauftragte führt ein Register der automatisiert geführten Dateien, in denen personenbezogene Daten gespeichert werden. **2**Das gilt nicht für die Dateien 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.	(1) **1**Der Bundesbeauftragte für den Datenschutz erstattet dem Deutschen Bundestag alle zwei Jahre einen Tätigkeitsbericht. **2Er unterrichtet den Deutschen Bundestag und die Öffentlichkeit über wesentliche Entwicklungen des Datenschutzes im öffentlichen und nicht-öffentlichen Bereich.** (2) **1**Auf Anforderung des Deutschen Bundestages oder der Bundesregierung hat der Bundesbeauftragte Gutachten zu erstellen und Berichte zu erstatten. **2**Auf Ersuchen des Deutschen Bundestages, des Petitionsausschusses, des Innenausschusses oder der Bundesregierung geht der Bundesbeauftragte ferner Hinweisen auf Angelegenheiten und Vorgänge des Datenschutzes bei den öffentlichen Stellen des Bundes nach. **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 Empfehlungen zur Verbesserung des Datenschutzes geben und sie in Fragen des Datenschutzes 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 Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind, sowie mit den Aufsichtsbehörden nach § 38 hin. **§ 38 Abs. 1 Satz 3 und 4 gilt entsprechend.**	*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 sowohl im öffentlichen als auch im nicht-öffentlichen Bereich zu unterrichten.* *Absatz 4 Satz 2 erstreckt die Amtshilferegelung des § 38 Abs. 1 Satz 3 und 4 für die Aufsichtsbehörden auf den Bundesbeauftragten für den Datenschutz.* *Nach § 4 d Abs. 1 und 2 in Verbindung mit § 4 f Abs. 1 Satz 1 entfällt aufgrund der obligatorischen Bestellung eines behördlichen Datenschutzbeauftragten die Meldepflicht im öffentlichen Bereich. Adressat der Verpflichtung nach § 4 g Abs. 2 ist im öffentlichen Bereich ausschließlich der Datenschutzbeauftragte. Die Notwendigkeit zur Führung eines Registers beim Bundesbeauftragten für den Datenschutz nach Absatz 5 a.F. entfällt daher.*

Dritter Abschnitt

Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen

Erster Unterabschnitt
Rechtsgrundlagen der Datenverarbeitung

§ 27 a.F. Anwendungsbereich	§ 27 n.F. Anwendungsbereich	***Begründung:***
(1) Die Vorschriften dieses Abschnittes finden Anwendung, soweit personenbezogene Daten in oder aus Dateien geschäftsmäßig oder für berufliche oder gewerbliche Zwecke verarbeitet oder genutzt 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. In den Fällen der Nummer 2 Buchstabe a gelten anstelle des § 38 die §§ 18, 21 und 24 bis 26. (2) Die Vorschriften dieses Abschnittes gelten nicht für die Verarbeitung und Nutzung personenbezogener Daten in Akten, soweit es sich nicht um personenbezogene Daten handelt, die offensichtlich aus einer Datei entnommen worden sind.	(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 <u>nicht-automatisierten</u> 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. Dies gilt nicht, wenn die Erhebung, Verarbeitung oder Nutzung der Daten ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt. In den Fällen der Nummer 2 Buchstabe a gelten anstelle des § 38 die §§ 18, 21 und 24 bis 26. (2) Die Vorschriften dieses Abschnittes gelten nicht für die Verarbeitung und Nutzung personenbezogener Daten **außerhalb von <u>nicht-automatisierten</u> Dateien**, soweit es sich nicht um personenbezogene Daten handelt, die offensichtlich aus einer **automatisierten Verarbeitung** entnommen worden sind.	*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.* *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. Datenspeicherung, -übermittlung und -nutzung für eigene Zwecke	§ 28 n.F. Daten**erhebung**, **-verarbeitung** und –nutzung für eigene Zwecke	***Begründung:***
(1) **1**Das Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig	(1) Das **Erheben**, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig	*Zu Absatz 1 Satz 1:* *Absatz 1 Satz 1 bedurfte der Ergänzung durch den Begriff der Erhebung, da Artikel 2 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.* *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 dem Ersatz 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 Abwägung der schutzwürdigen Interessen des Betroffenen mit dem berechtigten Interesse der verantwortlichen Stelle stattfinden muß. 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.*
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**,	
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 Nutzung überwiegt, oder	
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 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 Verarbeitung oder Nutzung **gegenüber dem berechtigten Interesse der verantwortlichen Stelle** offensichtlich überwiegt.	
4. wenn es im Interesse der speichernden Stelle zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluß der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.	**Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen.**	*Zu Absatz 1 Satz 2:* *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 diesen 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*
2Die Daten müssen nach Treu und Glauben und auf rechtmäßige Weise erhoben werden.		

§ 28 a.F. (Forts.)	§ 28 n.F. (Forts.)	***Begründung (Forts.):***
	(2) Für einen anderen Zweck dürfen sie nur unter den Voraussetzungen des Absatzes 1 Nr. 2 und 3 übermittelt oder genutzt werden.	*zu informieren. Dies setzt voraus, daß bereits bei der Erhebung der Zweck festliegen muß.*
(2) **1**Die Übermittlung oder Nutzung ist auch zulässig	(**3**) **1**Die Übermittlung oder Nutzung **für einen anderen Zweck** ist auch zulässig:	*Zu Absatz. 2:*
1.a) soweit es zur Wahrung berechtigter Interessen eines Dritten oder öffentlicher Interessen erforderlich ist oder	1. soweit es zur Wahrung berechtigter Interessen eines Dritten oder	*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 Zweckbindung 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 vorstellbar sind, konnte der Verweis auf Absatz 1 Nr. 2 und 3 beschränkt werden.*
	2. **zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten** 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 Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat.	3. **für Zwecke der Werbung, der Markt- oder Meinungsforschung,** wenn es sich um listenmäßig oder sonst zusammengefaßte Daten über Angehörige einer Personengruppe handelt, die sich auf a) eine Angabe über die Zugehörigkeit des Betroffenen zu dieser Personengruppe, b) Berufs-, Branchen- oder Geschäftsbezeichnung, c) Namen, d) Titel, e) akademische Grade, f) Anschrift, 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	*Zu Absatz 3:* *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 sowie 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 verdeutlicht. 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 1aE 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 nach § 3 Abs. 9, und damit auch für Gesundheitsdaten, eine enge Verwendungsbeschränkung vorsieht.*
2In den Fällen des Buchstabens b kann im allgemeinen davon ausgegangen werden, daß dieses Interesse besteht, wenn im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses 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	4. wenn es im Interesse einer Forschungseinrichtung zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluß der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.	
	2In 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.	

§ 28 a.F. (Forts.)	§ 28 n.F. (Forts.)	***Begründung (Forts.):***
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 Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.		*Zu Absatz 4:*
		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.
(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**Widerspricht 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.	(**4**) Widerspricht der Betroffene bei der **verantwortlichen** Stelle der Nutzung oder Übermittlung seiner Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung, ist eine Nutzung oder Übermittlung für diese Zwecke unzulässig. **Der Betroffene ist bei der Ansprache zum Zwecke der Werbung oder der Markt- oder Meinungsforschung über die verantwortliche Stelle sowie über das Widerspruchsrecht nach Satz 1 zu unterrichten.** Widerspricht der Betroffene bei **dem Dritten, dem die Daten nach Absatz 3 übermittelt werden,** der Verarbeitung oder Nutzung zum Zwecke der Werbung oder der Markt- oder Meinungsforschung, hat dieser die Daten für diese Zwecke zu sperren.	*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.*
		Zu Absatz 5:
		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.
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**) **1Der 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.	

	(6) Das Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten nach § 3 Abs. 9 für eigene Geschäftszwecke ist zulässig, soweit nicht der Betroffene nach Maßgabe des § 4a Abs. 3 eingewilligt hat, wenn **1. dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu geben,** **2. es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,** **3. dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Erhebung, Verarbeitung oder Nutzung überwiegt, oder** **4. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluß der Erhebung, Verarbeitung und Nutzung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.** **(7) Das Erheben von besonderen Arten personenbezogener Daten nach § 3 Abs. 9 ist ferner zulässig, wenn dies zum Zwecke der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen. Die Verarbeitung und Nutzung von Daten zu den in Satz 1 genannten Zwecken richtet sich nach den für die in Satz 1 genannten Personen geltenden Geheimhaltungspflichten. Werden zu einem in Satz 1 genannten Zweck Daten über die Gesundheit von Personen durch Angehörige eines anderen als in § 203 Abs. 1 und 3 des 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) Für einen anderen Zweck dürfen die besonderen Arten personenbezogener Daten nach § 3 Abs. 9 nur unter den Voraussetzungen des Absatzes 6 Nr. 1 bis 4 oder Absatz 7 Satz 1 übermittelt oder genutzt werden. Eine Übermittlung oder Nutzung ist auch zulässig, wenn dies zur Abwehr von erheblichen Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten von erheblicher Bedeutung erforderlich ist.** **(9) Organisationen, die politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtet sind und keinen Erwerbszweck verfolgen, dürfen besondere Arten personenbezogener Daten nach § 3 Abs. 9 erheben, verarbeiten oder nutzen, soweit dies für die Tätigkeit der Organisation erforderlich ist. Dies gilt nur für personenbezogene Daten ihrer Mitglieder oder von Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßig Kontakte mit ihr unterhalten. Die Übermittlung dieser personenbezogenen Daten an Personen oder Stellen außerhalb der Organisation ist nur unter den Voraussetzungen des § 4 a Abs. 3 zulässig. Absatz 3 Nr. 2 gilt entsprechend.**	*Zu Absatz 6 bis 9:* *Die Absätze 6 bis 9 setzen Artikel 8 der Richtlinie um. Da Sonderregelungen für die Verwendung der in § 3 Abs. 9 genannten Arten personenbezogener Daten auf dem Gebiet des Arbeitsrechts – im Regelfall auf der Basis höchstrichterlicher Rechtsprechung – bestehen, war Artikel 8 Abs. 2 Buchstabe b der Richtlinie nicht umzusetzen.* *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.* *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.* *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.* *Absatz 9 setzt Artikel 8 Abs. 2 Buchstabe d der Richtlinie um.*

§ 29 a.F. Geschäftsmäßige Datenspeicherung zum Zwecke der Übermittlung	§ 29 n.F. Geschäftsmäßige Daten**erhebung und** –speicherung zum Zwecke der Übermittlung	***Begründung:***
(1) Das geschäftsmäßige Speichern oder Verändern personenbezogener Daten zum Zwecke der Übermittlung ist zulässig, wenn	(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	*Zu Absatz 1:* *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.*
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. § 28 Abs. 1 Satz 2 ist anzuwenden.	1. kein Grund zu der Annahme besteht, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Erhebung, Speicherung oder Veränderung hat, oder 2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die **verantwortliche** Stelle sie veröffentlichen dürfte, es sei denn, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Erhebung, Speicherung oder Veränderung offensichtlich überwiegt. § 28 Abs. 1 Satz 2 ist anzuwenden.	*Zu Absatz 2:* *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 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, 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.*
(2) **1**Die Übermittlung ist zulässig, wenn	(2) **1**Die Übermittlung **im Rahmen der Zwecke nach Absatz 1** ist zulässig, wenn	
1. a) der Empfänger ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat oder 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.	1. a) **der Dritte, dem die Daten übermittelt werden,** ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat oder b) es sich um listenmäßig oder sonst zusammengefaßte Daten nach § 28 Abs. **3** Nr. 3 handelt, die für Zwecke der Werbung oder der Markt- oder Meinungsforschung übermittelt werden sollen, und 2. kein Grund zu der Annahme besteht, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat.	
2§ 28 Abs. 2 Nr. 1 Satz 2 gilt entsprechend. Bei der Übermittlung nach Nummer 1 Buchstabe a sind die Gründe für das Vorliegen eines berechtigten Interesses und die Art und Weise ihrer glaubhaften Darlegung von der übermittelnden Stelle aufzuzeichnen. **3**Bei der Übermittlung im automatisierten Abrufverfahren obliegt die Aufzeichnungspflicht dem Empfänger.	**2**§ 28 Abs. **3** Satz 2 gilt entsprechend. Bei der Übermittlung nach Nummer 1 Buchstabe a sind die Gründe für das Vorliegen eines berechtigten Interesses und die Art und Weise ihrer glaubhaften Darlegung von der übermittelnden Stelle aufzuzeichnen. Bei der Übermittlung im automatisierten Abrufverfahren obliegt die Aufzeichnungspflicht dem **Dritten, dem die Daten übermittelt werden**.	

§ 29 a.F. (Forts.)	**§ 29 n.F. (Forts.)**	***Begründung (Forts.):***
	(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 zugrundeliegenden 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.	*Zu Absatz 3:* *§ 10 Telekommunikationsdiensteunternehmen-Datenschutzverordnung (TDSV) erlaubt, daß sog. Dienstanbieter, 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 Verzeichnissen 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.*
(3) Für die Verarbeitung oder Nutzung der übermittelten Daten gilt § 28 Abs. 3 und 4.	(4) Für die Verarbeitung oder Nutzung der übermittelten Daten gilt § 28 Abs. **4** und **5**.	*Der neue Absatz 3 schafft nun Rechtsklarheit insofern, als er sicherstellt, daß der Wille von Betroffenen, nicht eingetragen zu werden, von jedem potentiellen Herausgeber entsprechender Verzeichnisse dahingehend zu respektieren ist, daß die Aufnahme in Adreß- u.ä. Verzeichnisse zu unterbleiben hat oder bei der Übernahme in Verzeichnisse 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.*
	(5) § 28 Abs. 6 bis 9 gelten entsprechend.	*Zu Absatz 4:* *Die geänderten Verweise in Absatz 4 sind Folgeänderungen im Zusammenhang mit der Schaffung eines neuen Absatzes 2 in § 28.* *Zu Absatz 5:* *Absatz 5 stellt sicher, daß die Restriktionen für die Erhebung, Verarbeitung und Nutzung sensitiver Daten auch im Anwendungsbereich von § 29 gelten.*

§ 30 a.F. Geschäftsmäßige Datenspeicherung zum Zwecke der Übermittlung in anonymisierter Form	§ 30 n.F. Geschäftsmäßige Daten**erhebung und** –speicherung zum Zwecke der Übermittlung in anonymisierter Form	***Begründung:***
(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 Speicherung oder zu wissenschaftlichen Zwecken erforderlich ist.	(1) **1**Werden personenbezogene Daten geschäftsmäßig **erhoben und** gespeichert, um sie in anonymisierter Form zu übermitteln, sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. **2**Diese Merkmale dürfen mit den Einzelangaben nur zusammengeführt werden, soweit 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.* *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.* *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.* *Zu Absatz 5:* *Auf die Begründung zu § 29 Abs. 5 wird 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 schutzwürdige Interesse des Betroffenen an dem Ausschluß der Veränderung offensichtlich überwiegt.	(2) Die Veränderung personenbezogener Daten ist zulässig, wenn 1. kein Grund zu der Annahme besteht, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Veränderung hat, oder 2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die **verantwortliche** Stelle sie veröffentlichen dürfte, **soweit nicht** das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Veränderung offensichtlich überwiegt.	
(3) Die personenbezogenen Daten sind zu löschen, wenn ihre Speicherung unzulässig ist.	(3) Die personenbezogenen Daten sind zu löschen, wenn ihre Speicherung unzulässig ist.	
(4) Die §§ 29, 33 bis 35 gelten nicht.	(4) § 29 gilt nicht. **(5) § 28 Abs. 6 bis 9 gelten entsprechend.**	

§ 31 Besondere Zweckbindung Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.	*Hinweis: Vorschrift ist unverändert.*	

§ 32 a.F. 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. (2) **1**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 berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen, 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. **2**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 Datenverarbeitungsanlagen, 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.	Hinweis: Die Vorschrift wurde vollständig **aufgehoben**.	***Begründung:*** *Die Aufhebung von § 32 a.F. ist eine Folgeänderung im Zusammenhang mit den neu geschaffenen Vorschriften der §§ 4 d und 4 e.*

Zweiter Unterabschnitt
Rechte des Betroffenen

§ 33 a.F. Benachrichtigung des Betroffenen	§ 33 n.F. Benachrichtigung des Betroffenen	***Begründung:***
(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 geschäftsmäßig zum Zwecke der Übermittlung gespeichert, ist der Betroffene von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen.	(1) Werden erstmals personenbezogene Daten für eigene Zwecke **ohne Kenntnis des Betroffenen** gespeichert, ist der Betroffene von der Speicherung, der Art der Daten, **der Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und der Identität der verantwortlichen Stelle** zu benachrichtigen. Werden personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung **ohne Kenntnis des Betroffenen** gespeichert, ist der Betroffene von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen. **Der Betroffene ist in den Fällen der Sätze 1 und 2 auch über die Kategorien von Empfängern zu unterrichten, soweit er nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muß.**	*Zu Absatz 1:* *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.*

§ 33 a.F. Benachrichtigung des Betroffenen	§ 33 n.F. Benachrichtigung des Betroffenen	***Begründung (Forts.):***
		Zu Absatz 2 Nr. 2:
(2) Eine Pflicht zur Benachrichtigung besteht nicht, wenn	(2) Eine Pflicht zur Benachrichtigung besteht nicht, wenn	*Die bisher geltende Ausnahme von der Benachrichtigung in Absatz 2 Nr. 2 war aufgrund des in Artikel 11 Abs.2 der Richtlinie vorgesehenen Gedankens des Absehens von der Benachrichtigung aus Gründen der Unverhältnismäßigkeit entsprechend einzuschränken.*
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 Datenschutzkontrolle dienen,	2. die Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich der Datensicherung oder der Datenschutzkontrolle dienen **und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde,**	*Zu Absatz 2 Satz 1 Nr. 4:*
3. die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheimgehalten werden müssen,	3. die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheimgehalten werden müssen, **4. die Speicherung oder Übermittlung durch Gesetz ausdrücklich vorgesehen ist,**	*Durch die neu eingefügte Nummer 4 wird der Ausnahmekatalog des Absatz 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 Speicherung oder Übermittlung für Zwecke der wissenschaftlichen Forschung erforderlich ist und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde,	
4. die zuständige öffentliche Stelle gegenüber der speichernden Stelle festgestellt hat, daß das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,	**6.** die 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,	
5. die Daten in einer Datei gespeichert werden, die nur vorübergehend vorgehalten und innerhalb von drei Monaten nach ihrer Erstellung gelöscht wird,	**7.** die Daten für eigene Zwecke gespeichert sind und	*Zu Absatz 2 Satz 1 Nr. 5:*
6. die Daten für eigene Zwecke gespeichert sind und a) aus allgemein zugänglichen Quellen entnommen sind oder	a) aus allgemein zugänglichen Quellen entnommen sind **und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist,** oder	*Hinsichtlich der Aufhebung von Absatz 2 Nr. 5 a.F. wird auf die Begründung zur Aufhebung von § 18 Abs. 3 verwiesen.*
b) die Benachrichtigung die Geschäftszwecke der speichernden Stelle erheblich gefährden würde, es sei denn, daß das Interesse an der Benachrichtigung die Gefährdung überwiegt, oder	b) die Benachrichtigung die Geschäftszwecke der **verantwortlichen** Stelle erheblich gefährden würde, es sei denn, daß das Interesse an der Benachrichtigung die Gefährdung überwiegt, oder	*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.*
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, 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	*Zu Absatz 2 Satz 1 Nr. 7 a und 8:*
b) es sich um listenmäßig oder sonst zusammengefaßte Daten handelt (§ 29 Abs. 2 Nr. 1 Buchstabe b).	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.*
	Die verantwortliche Stelle legt schriftlich fest, unter welchen Voraussetzungen von einer Benachrichtigung nach Absatz 2 Nrn. 2 bis 7 abgesehen wird.	*Zu Absatz 2 Satz 2:* *Durch Absatz 2 Satz 2 wird das Erfordernis der „geeigneten Garantien„ gemäß Artikel 11 Abs. 2 Satz 2 der Richtlinie umgesetzt. Der betriebliche Datenschutzbeauftragte wirkt auf die Einhaltung dieser Vorschrift hin.*

§ 34 a.F. Auskunft an den Betroffenen	§ 34 n.F. Auskunft an den Betroffenen	***Begründung:***
(1) **1**Der Betroffene kann Auskunft verlangen über 1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf Herkunft und Empfänger beziehen, 2. den Zweck der Speicherung und 3. Personen und Stellen, an die seine Daten regelmäßig übermittelt werden, wenn seine Daten automatisiert verarbeitet werden. **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 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**Auskunft über Herkunft und Empfänger kann der Betroffene nur verlangen, wenn er begründete Zweifel an der Richtigkeit der Daten geltend macht. **3**§ 38 Abs. 1 ist mit der Maßgabe anzuwenden, daß die Aufsichtsbehörde im Einzelfall die Einhaltung von Satz 1 überprüft, wenn der Betroffene begründet darlegt, daß die Auskunft nicht oder nicht richtig erteilt worden 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. (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 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.	(1) Der Betroffene kann Auskunft verlangen über 1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf **die** Herkunft dieser Daten beziehen, **2. Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben werden,** und 3. den Zweck der Speicherung. **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, **sofern 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 **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.** (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. **3 und** 6 nicht zu benachrichtigen ist. (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 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.	*Zu Absatz 1:* *Durch die Neufassung wird Artikel 12 Buchstabe a, 1. Spiegelstrich der Richtlinie umgesetzt.* *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 Auskunftsrecht nach Artikel 13 Buchstabe g der Richtlinie. Der Schutz der „Rechte und Freiheiten anderer Personen„ umfaßt auch das Geschäftsgeheimnis.* *Zu Absatz 2:* *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.* *Zu Absatz 4:* *Anders als im Rahmen der Benachrichtigung sind im Rahmen der Auskunft Ausnahmen in den Fällen des § 33 Abs. 2 Nr. 2, 4 und 5 nicht sachgerecht. Die Verweisung in § 33 Abs. 4 war dementprechend zu begrenzen.*

§ 35 a.F. Berichtigung, Löschung und Sperrung von Daten	§ 35 n.F. Berichtigung, Löschung und Sperrung von Daten	***Begründung:***
(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind.	(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind.	*Absatz 2 Satz 2 Nr. 2 ist um die Merkmale von Artikel 8 der Richtlinie ergänzt.Im Hinblick auf den Ersatz der Wörter „speichernde Stelle„ durch die Wörter „verantwortliche Stelle„ wird auf die Begründung zu § 3 Abs. 7 verwiesen.*
(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	*Durch die Änderungen in Absatz 2 Satz 2 Nr. 4 wird sicher gestellt, dass bei Daten, die geschäftsmäßig zum Zwecke der Übermittlung verarbeitet werden, jeweils nach vier Jahren eine Überprüfung ihrer Erforderlichkeit erfolgt.*
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,	1. ihre Speicherung unzulässig ist, 2. es sich um Daten über **die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit, über Gesundheit oder das Sexualleben**, strafbare Handlungen oder Ordnungswidrigkeiten handelt und ihre Richtigkeit von der **verantwortlichen** Stelle nicht bewiesen werden kann,	*Hinsichtlich der Einfügung von Absatz 5 wird auf die Begründung zu § 20 Abs. 5 verwiesen.*
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 Prüfung am Ende des fünften Kalenderjahres nach ihrer erstmaligen Speicherung ergibt, daß eine längerwährende Speicherung nicht erforderlich ist.	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 Prüfung jeweils am Ende des vierten Kalenderjahres beginnend mit ihrer erstmaligen Speicherung ergibt, daß eine längerwährende Speicherung nicht erforderlich ist.	
(3) An die Stelle einer Löschung tritt eine Sperrung, soweit 1. im Falle des Absatzes 2 Nr. 3 oder 4 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. im Falle des Absatzes 2 Nr. 3 einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen, 2. Grund zu der Annahme besteht, daß durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder 3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.	
(4) Personenbezogene Daten sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen läßt.	(4) Personenbezogene Daten sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen läßt.	
	(5) Personenbezogene Daten dürfen nicht für eine automatisierte Verarbeitung oder Verarbeitung in <u>nicht-automatisierten</u> 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. <u>Satz 1 gilt nicht, wenn eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung verpflichtet.</u>	

§ 35 a.F. (Forts.)	§ 35 n.F. (Forts.)	***Begründung (Forts.):***
(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. (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 Daten zur Speicherung weitergegeben werden, wenn dies zur Wahrung der schutzwürdigen 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 Beweisnot oder aus sonstigen im überwiegenden 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**) **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**) Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu verständigen, denen im Rahmen einer Datenübermittlung diese Daten zur Speicherung weitergegeben werden, wenn dies **keinen unverhältnismäßigen Aufwand erfordert und schutzwürdige Interessen des Betroffenen nicht entgegenstehen.** (**8**) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn 1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der **verantwortlichen** Stelle oder eines Dritten liegenden Gründen unerläßlich ist und 2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.	*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.* *Die Änderung in Absatz 8 Nr. 1 ist eine Folgeänderung im Zusammenhang mit dem Ersatz des Begriffs der speichernden Stelle durch den der verantwortlichen Stelle (vgl. hierzu die Begründung zu § 3 Abs. 7).*

Dritter Unterabschnitt **Beauftragter für den Datenschutz, Aufsichtsbehörde**	**Dritter Unterabschnitt** **Aufsichtsbehörde**	***Begründung:*** *Die Regelungen über den betrieblichen Datenschutzbeauftragten wurden im Dritten Abschnitt aufgehoben und finden sich nunmehr in den §§ 4 f und 4 g. Die Überschrift des Dritten Unterabschnitts war daher anzupassen.*
§ 36 a.F. 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. (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 Erfüllung seiner Aufgaben erforderlich ist, Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen.	Hinweis: Die Vorschrift wurde vollständig **aufgehoben**.	***Begründung:*** *Die Aufhebung von § 36 ist eine Folgeänderung im Zusammenhang mit der neu geschaffenen Vorschrift des § 4 f.*

§ 37 a.F.	Hinweis:	***Begründung:***
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 1. die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen; zu diesem Zweck ist er über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten, 2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderen Vorschriften über den Datenschutz, bezogen auf die besonderen Verhältnisse in diesem Geschäftsbereich und die sich daraus ergebenden besonderen 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 Datenverarbeitungsanlagen, 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.	Die Vorschrift wurde vollständig **aufgehoben**.	*Die Aufhebung von § 37 ist eine Folgeänderung im Zusammenhang mit der neu geschaffenen Vorschrift des § 4 g.*

§ 38 a.F. Aufsichtsbehörde	§ 38 n.F. Aufsichtsbehörde	***Begründung:***
(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 dieser Vorschriften durch nicht-öffentliche Stellen verletzt ist, insbesondere wenn es der Betroffene selbst begründet darlegt.	(1) Die Aufsichtsbehörde kontrolliert die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus **nicht-automatisierten** Dateien regeln **einschließlich des Rechts der Mitgliedstaaten in den Fällen des § 1 Abs. 5. ___ Die Aufsichtsbehörde darf die von ihr gespeicherten Daten nur für Zwecke der Aufsicht verarbeiten und nutzen; § 14 Abs. 2 Nrn. 1 bis 3, 6 und 7 gelten entsprechend. Insbesondere darf die Aufsichtsbehörde zum Zweck der Aufsicht Daten an andere Aufsichtsbehörden übermitteln. Sie leistet den Aufsichtsbehörden anderer Mitgliedstaaten der Europäischen Union auf Ersuchen ergänzende Hilfe (Amtshilfe). ___ Stellt die Aufsichtsbehörde einen Verstoß gegen dieses Gesetz odere andere Vorschriften über den Datenschutz fest, so ist sie befugt, die Betroffenen hierüber zu unterrichten, den Verstoß bei den für die Verfolgung oder Ahndung zuständigen Stellen anzuzeigen sowie bei schwerwiegenden Verstößen die Gewerbeaufsichtsbehörde zur Durchführung gewerberechtlicher Maßnahmen zu unterrichten. Sie veröffentlicht regelmäßig, spätestens alle zwei Jahre, einen Tätigkeitsbericht. § 21 Satz 1 und § 23 Abs. 5 Satz 4 bis 7 gilt entsprechend.**	*Zu Absatz 1:* *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 Übereinstimmung 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 dienen der Sicherung der funktionalen Unabhängigkeit der Aufsichtsbehörden. Es wird auf der einen Seite die Zweckbindung der von der Aufsichtsbehörde gespeicherten Daten festgelegt, andererseits die notwendigen Datenübermittlungen der Aufsichtsbehörde an andere Stellen näher geregelt.* *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.*
(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 Vorschriften über den Datenschutz, soweit diese die Verarbeitung oder Nutzung personenbezogener Daten in oder aus Dateien regeln. **2**Die Aufsichtsbehörde führt das Register nach § 32 Abs. 2. **3**Das Register kann von jedem eingesehen werden.	(2) **Die Aufsichtsbehörde führt ein Register der nach § 4 d meldepflichtigen automatisierten Verarbeitungen mit den Angaben gemäß § 4 e Satz 1**. Das Register kann von jedem eingesehen werden. Das Einsichtsrecht erstreckt sich nicht auf die Angaben nach § 4 e Satz 1 Nr. 9 sowie auf die Angabe der zugriffsberechtigten Personen.	
(3) **1**Die der Prüfung 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.	(3) Die der Prüfung unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen haben der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen. Der Auskunftspflichtige kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 der Zivilprozeßordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Der Auskunftspflichtige ist darauf hinzuweisen.	

§ 38 a.F. (Forts.)	§ 38 n.F. (Forts.)	***Begründung (Forts):***
(4) 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. 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. Der Auskunftspflichtige hat diese Maßnahmen zu dulden.	(4) 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. Sie können geschäftliche Unterlagen, insbesondere die Übersicht nach **§ 4 g Abs. 2 Satz 1** sowie die gespeicherten personenbezogenen Daten und die Datenverarbeitungsprogramme, einsehen. § 24 Abs. 6 gilt entsprechend. Der Auskunftspflichtige hat diese Maßnahmen zu dulden.	*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.*
(5) Zur Gewährleistung des Datenschutzes nach diesem Gesetz und anderen Vorschriften über den Datenschutz, soweit diese die Verarbeitung oder Nutzung personenbezogener Daten in oder aus Dateien regeln, kann die Aufsichtsbehörde anordnen, daß im Rahmen der Anforderungen nach § 9 Maßnahmen zur Beseitigung festgestellter technischer oder organisatorischer Mängel getroffen werden. Bei schwerwiegenden Mängeln dieser Art, insbesondere, wenn sie mit besonderer Gefährdung des Persönlichkeitsrechts verbunden sind, kann sie den Einsatz einzelner Verfahren untersagen, wenn die Mängel entgegen der Anordnung nach Satz 1 und trotz der Verhängung eines Zwangsgeldes nicht in angemessener Zeit beseitigt werden. Sie kann die Abberufung des Beauftragten für den Datenschutz verlangen, wenn er die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit nicht besitzt.	(5) Zur Gewährleistung des Datenschutzes nach diesem Gesetz und anderen Vorschriften über den Datenschutz, soweit diese die **automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung personenbezogener Daten in oder aus <u>nicht-automatisierten</u> Dateien** regeln, kann die Aufsichtsbehörde anordnen, daß im Rahmen der Anforderungen nach § 9 Maßnahmen zur Beseitigung festgestellter technischer oder organisatorischer Mängel getroffen werden. Bei schwerwiegenden Mängeln dieser Art, insbesondere, wenn sie mit besonderer Gefährdung des Persönlichkeitsrechts verbunden sind, kann sie den Einsatz einzelner Verfahren untersagen, wenn die Mängel entgegen der Anordnung nach Satz 1 und trotz der Verhängung eines Zwangsgeldes nicht in angemessener Zeit beseitigt werden. Sie kann die Abberufung des Beauftragten für den Datenschutz verlangen, wenn er die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit nicht besitzt.	*Zu Absatz 2:* *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 Regelungen 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.*
(6) Die Landesregierungen oder die von ihnen ermächtigten Stellen bestimmen die für die Überwachung der Durchführung des Datenschutzes im Anwendungsbereich dieses Abschnittes zuständigen Aufsichtsbehörden.	(6) Die Landesregierungen oder die von ihnen ermächtigten Stellen bestimmen die für die Überwachung der Durchführung des Datenschutzes im Anwendungsbereich dieses Abschnittes zuständigen Aufsichtsbehörden.	*Zu Absatz 4:* *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.*
(7) Die Anwendung der Gewerbeordnung auf die den Vorschriften dieses Abschnitts unterliegenden Gewerbebetriebe bleibt unberührt.	(7) Die Anwendung der Gewerbeordnung auf die den Vorschriften dieses Abschnitts unterliegenden Gewerbebetriebe bleibt unberührt.	*Zu Absatz 5:* *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 personenbezogener Daten oder die Verarbeitung personenbezogener Daten in oder aus <u>nicht-automatisierten Dateien</u>„ auf die Begründung zu § 3 Abs. 2 verwiesen.*

	§ 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 Verhaltensregeln zur Förderung der Durchführung von datenschutzrechtlichen Regelungen der zuständigen Aufsichtsbehörde unterbreiten.** **(2) Die Aufsichtsbehörde <u>überprüft</u> die Vereinbarkeit der ihr <u>unterbreiteten</u> Entwürfe mit dem geltenden Datenschutzrecht ___.**	***Begründung:*** *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 Vereinigungen erhalten die Möglichkeit, von ihnen erarbeitete Verhaltensregeln der Aufsichtsbehörde zur Überprüfung vorzulegen. Die Entwürfe sind in rechtlicher, technischer und organisatorischer Hinsicht ausreichend zu begründen und auf Verlangen der Aufsichtsbehörde zu erläutern.* *Die Verpflichtung der Aufsichtsbehörde zur Überprüfung ihr vorgelegter Entwürfe anhand des geltenden Datenschutzrechts gemäß Absatz 2 soll verhindern, daß Berufsverbände und die anderen in Absatz 1 genannten Vereinigungen sich interne Verhaltensregeln geben, die im Widerspruch zu den gesetzlichen Regelungen stehen.*

Vierter Abschnitt
Sondervorschriften

§ 39 Zweckbindung bei personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen (1) 1Personenbezogene 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. 2In die Übermittlung an eine nicht-öffentliche Stelle muß die zur Verschwiegenheit verpflichtete Stelle einwilligen. (2) Für einen anderen Zweck dürfen die Daten nur verarbeitet oder genutzt werden, wenn die Änderung des Zwecks durch besonderes Gesetz zugelassen ist.	§ 39 Zweckbindung bei personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen (1) 1Personenbezogene 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. 2In die Übermittlung an eine nicht-öffentliche Stelle muß die zur Verschwiegenheit verpflichtete Stelle einwilligen. (2) Für einen anderen Zweck dürfen die Daten nur verarbeitet oder genutzt werden, wenn die Änderung des Zwecks durch besonderes Gesetz zugelassen ist.	***Begründung:*** *Die Änderung in Absatz 1 Satz 1 ist eine Folgeänderung im Zusammenhang mit dem Ersatz des Begriffs der speichernden Stelle durch den der verantwortlichen Stelle (vgl. hierzu die Begründung zu § 3 Abs. 7).*

§ 40 a.F. Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen	§ 40 n.F. Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen	***Begründung:***
(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.	
(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.		*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.*
(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 bestimmten oder bestimmbaren Person zugeordnet werden können. **3**Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert.	(**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 bestimmten oder bestimmbaren Person zugeordnet werden können. **3**Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert.	
(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.	(**3**) Die wissenschaftliche Forschung betreibenden Stellen dürfen personenbezogene Daten nur veröffentlichen, wenn 1. der Betroffene eingewilligt hat oder 2. dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerläßlich ist.	

§ 41 a.F. Verarbeitung und Nutzung personenbezogener Daten durch die Medien	§ 41 n.F. **Erhebung,** Verarbeitung und Nutzung personenbezogener Daten durch die Medien	***Begründung:***
(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)** <Fassung wird derzeit überarbeitet>	___
(2) Führt die journalistisch-redaktionelle Verarbeitung oder Nutzung personenbezogener Daten durch die Deutsche Welle zur Veröffentlichung von Gegendarstellungen des Betroffenen, so sind diese Gegendarstellungen zu den gespeicherten Daten zu nehmen und für dieselbe Zeitdauer aufzubewahren wie die Daten selbst.	(2) Führt die journalistisch–redaktionelle **Erhebung,** Verarbeitung oder Nutzung personenbezogener Daten durch die Deutsche Welle zur Veröffentlichung von Gegendarstellungen des Betroffenen, so sind diese Gegendarstellungen zu den gespeicherten Daten zu nehmen und für dieselbe Zeitdauer aufzubewahren wie die Daten selbst.	

§ 41 a.F. (Forts.)	§ 41 n.F. (Forts.)	***Begründung (Forts.):***
(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 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.	*Zu Absatz 4:* *Der Kreis der auf die Deutsche Welle anwendbaren Vorschriften des Bundesdatenschutzgesetzes war nach Maßgabe des Artikels 9 der Richtlinie zu erweitern.*
(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 38 a.** **2**Anstelle der §§ 24 bis 26 gilt § 42, auch soweit es sich um Verwaltungsangelegenheiten handelt.	

§ 42 a.F.	§ 42 n.F.	***Begründung:***
Datenschutzbeauftragter der Deutschen Welle	Datenschutzbeauftragte**r** der Deutschen Welle	*Die Änderungen in Absatz 5 Satz 2 sind Folgeänderungen im Zusammenhang mit der Schaffung einheitlicher Vorschriften für den internen Datenschutzbeauftragten (§§ 4 f und 4 g). Diese Regelungen über den internen Datenschutzbeauftragten, die erstmals auch für den behördlichen Bereich Anwendung finden, gelten damit ausdrücklich im Bereich der Deutschen Welle. Hierdurch erfährt insbesondere auch der Datenschutzbeauftragte der Deutschen Welle eine deutliche Aufwertung.*
(1) **1**Die Deutsche Welle bestellet 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 Welle 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 Welle 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. **§§ 4 f und 4 g bleiben unberührt.**	

Fünfter Abschnitt
Schlußvorschriften

§ 43 a.F. Strafvorschriften	§ 43 n.F. Strafvorschriften	***Begründung:***
(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. (2) Ebenso wird bestraft, wer 1. die Übermittlung von durch dieses Gesetz geschützten personenbezogenen Daten, die nicht offenkundig sind, durch unrichtige Angaben erschleicht, 2. entgegen § 16 Abs. 4 Satz 1, § 28 Abs. 4 Satz 1, auch in Verbindung mit § 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.	(1) Wer unbefugt personenbezogene Daten, die nicht offenkundig sind, 1. **erhebt** oder **verarbeitet**, 2. zum Abruf mittels automatisierten Verfahrens bereithält oder 3. abruft oder sich oder einem anderen aus **automatisierten Verarbeitungen oder <u>nicht-automatisierten</u>** Dateien verschafft, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft. (2) Ebenso wird bestraft, wer 1. die Übermittlung von personenbezogenen Daten, die nicht offenkundig sind, durch unrichtige Angaben erschleicht, 2. 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 3. 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) 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. **Antragsberechtigt sind der Betroffene, <u>die verantwortliche Stelle,</u> der Bundesbeauftragte für den Datenschutz oder die Aufsichtsbehörde.**	*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 Zusammenhang mit der Einfügung eines neuen Absatzes 3 in § 29.* *Die Änderung der Verweise in Absatz 2 Nr. 3 ist eine Folgeänderung im Zusammenhang mit der Aufhebung von § 40 Abs. 2 a.F.* *Der Zusatz in Absatz 4 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. <u>Die Aufnahme der verantwortlichen Stelle ist sachgerecht, damit sich diese gegen einen Mißbrauch der von ihr gespeicherten Daten zur Wehr setzen kann.</u>*

§ 44 a.F.	§ 44 n.F.	***Begründung:***
Bußgeldvorschriften	Bußgeldvorschriften	*Zu Absatz 1 Nr. 2:*
(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig	(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig	*Die Änderung der Verweise in Absatz 1 Nr. 2 ist eine Folgeänderung im Zusammenhang mit der Aufhebung von § 32 sowie mit der Schaffung der neuen Vorschriften der §§ 4 d und 4 e.*
1. entgegen § 29 Abs. 2 Satz 3 oder 4 die dort bezeichneten Gründe oder die Art und Weise ihrer glaubhaften Darlegung nicht aufzeichnet,	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,	2. entgegen **§ 4 d Abs. 1 und 4**, auch in Verbindung mit **§ 4 e Satz 2**, eine Meldung nicht erstattet oder entgegen **§ 4 e Satz 1**, auch in Verbindung mit **§ 4 e Satz 2**, bei einer solchen Meldung die erforderlichen Angaben nicht, nicht richtig oder nicht vollständig mitteilt,	*Zu Absatz 1 Nr. 4:* *Die Änderung ist eine Folgeänderung im Zusammenhang mit der Einfügung eines neuen Absatzes 5 in § 35.*
3. entgegen § 33 Abs. 1 den Betroffenen nicht, nicht richtig oder nicht vollständig benachrichtigt,	3. entgegen § 33 Abs. 1 den Betroffenen nicht, nicht richtig oder nicht vollständig benachrichtigt,	*Zu Absatz 1 Nr. 5:* *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.*
4. entgegen § 35 Abs. 5 Satz 3 Daten ohne Gegendarstellung übermittelt,	4. entgegen § 35 Abs. 6 Satz 3 Daten ohne Gegendarstellung übermittelt,	*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.*
5. entgegen § 36 Abs. 1 einen Beauftragten für den Datenschutz nicht oder nicht rechtzeitig bestellt,	5. entgegen **§ 4 f 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 nicht duldet, oder	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 nicht duldet, oder	
7. einer vollziehbaren Anordnung nach § 38 Abs. 5 Satz 1 zuwiderhandelt.	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.	(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Deutsche Mark geahndet werden.	

	Sechster Abschnitt **Übergangsvorschriften**	
	§ 45 n.F. **Laufende Verwendungen** **Erhebungen, Verarbeitungen oder Nutzungen personenbezogener Daten, die zum Zeitpunkt des Inkrafttretens dieses Gesetzes bereits begonnen haben, sind binnen drei Jahren nach diesem Zeitpunkt mit den Vorschriften dieses Gesetzes in Übereinstimmung zu bringen.** **Soweit Vorschriften dieses Gesetzes in Rechtsvorschriften außerhalb des Anwendungsbereichs der in § 4 b Abs. 1 genannten Richtlinie zur Anwendung gelangen, sind Erhebungen, Verarbeitungen oder Nutzungen personenbezogener Daten, die zum Zeitpunkt des Inkrafttretens dieses Gesetzes bereits begonnen haben, binnen fünf Jahren nach diesem Zeitpunkt mit den Vorschriften dieses Gesetzes in Übereinstimmung zu bringen.**	***Begründung:*** *Die Vorschrift setzt Artikel 32 Abs. 2 der Richtlinie um. Er gestattet einen Anpassungszeitraum von maximal drei Jahren ab Inkrafttreten des Gesetzes für solche Erhebungen, 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 Richtlinie fallen, soweit die Vorschriften des BDSG in den jeweiligen bereichsspezifischen Gesetzen zur Anwendung gelangen. Hierfür enthält Satz 2 eine Sonderregelung.*

	§ 46 n.F. **Weitergeltung von Begriffsbestimmungen** **(1) Wird in besonderen Rechtsvorschriften des Bundes der Begriff Datei verwendet, ist Datei** **1. eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden kann (automatisierte Datei), oder** **2. jede sonstige Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen geordnet, umgeordnet und ausgewertet werden kann (nicht-automatisierte Datei).** **Nicht hierzu gehören Akten und Aktensammlungen, es sei denn, daß sie durch automatisierte Verfahren umgeordnet und ausgewertet werden können.** **(2) Wird in besonderen Rechtsvorschriften des Bundes der Begriff Akte verwendet, ist Akte jede amtlichen oder dienstlichen Zwecken dienende Unterlage, die nicht dem Dateibegriff des Absatzes 1 unterfällt; dazu zählen auch Bild- und Tonträger. Nicht hierunter fallen Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen.** **(3) Wird in besonderen Rechtsvorschriften des Bundes der Begriff Empfänger verwendet, ist Empfänger jede Person oder Stelle außerhalb der verantwortlichen Stelle. Empfänger sind nicht der Betroffene sowie diejenigen Personen und Stellen, die im Inland oder im Geltungsbereich der Rechtsvorschriften zum Schutz personenbezogener Daten der Mitgliedstaaten der Europäischen Union personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.**	***Begründung:*** *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 Datei, 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.* - 97 -

Anlage (zu § 9 Satz 1) a.F.	Anlage (zu § 9 Satz 1) n.F.	***Begründung:***
Werden personenbezogene Daten automatisiert verarbeitet, sind Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind,	Werden personenbezogene Daten automatisiert verarbeitet **oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere** Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten **oder Datenkategorien** geeignet sind,	*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 einzelnen gespeicherten Daten konkret gewährleistet wird.*
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)**,	*Im Einzelnen:* *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 sowie 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),	*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: Zutritt 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. 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 nicht unbefugt gelesen**, **kopiert,** verändert oder **entfernt werden können, und daß überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle)**,	
5. zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle),		

Anlage (zu § 9 Satz 1) a.F. (Forts.)	Anlage (zu § 9 Satz 1) n.F. (Forts.)	***Begründung (Forts.):***
6. zu gewährleisten, daß überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können (Übermittlungskontrolle),	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),	*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 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),	6. zu gewährleisten, daß personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),	
8. zu gewährleisten, daß personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),	**7. zu gewährleisten, daß personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),**	
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),	**8. zu gewährleisten, daß zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.**	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.*
10. die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).		*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.*

		Begründung (Forts.): 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 bisherige Fassung überzogene, nicht praktikable Anforderungen stellte. Gleichzeitig wurde der Anwendungsbereich der Nummer 5 um die nachträgliche Überprüfung und Feststellung der Veränderung oder Entfernung ergänzt.* 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 Regelfall zugelassenen Zweckänderungen Rechnung getragen werden soll.*