Begründung

A. Allgemeiner Teil

I. Ziel und Inhalt des Entwurfs

In der jüngeren Vergangenheit sind zunehmend Fälle des unberechtigten Handels mit personenbezogenen Daten bekannt geworden. Die Herkunft der Daten ist größtenteils nicht nachvollziehbar. Der bisherige Erlaubnistatbestand des § 28 Abs. 3 Satz 1 Nr. 3 des Bundesdatenschutzgesetzes hat sich dabei für die Herstellung der notwendigen Transparenz als besonders nachteilig erwiesen. Danach dürfen bestimmte personenbezogene Daten, wenn sie listenmäßig oder sonst zusammengefasst sind, für Zwecke der Werbung oder der Markt- oder Meinungsforschung, ohne Einwilligung der Betroffenen übermittelt oder genutzt werden. Die praktische Anwendung dieser Vorschrift hat dazu geführt, dass personenbezogene Daten der Bürgerinnen und Bürger weitläufig zum Erwerb oder zur Nutzung angeboten werden, ohne in jedem Fall die in der Vorschrift angelegten Anforderungen zu beachten. Personenbezogene Daten werden ohne Beachtung der Zweckbindung verarbeitet und mit weiteren Daten verknüpft und weiter übermittelt. Zudem hat sich das Verhältnis der Bürgerinnen und Bürger zur Werbung und Markt- oder Meinungsforschung seit der Einführung der Vorschrift im Bundesdatenschutzgesetz von 1977 gewandelt. Die gezielte Ansprache zum Zwecke der Werbung oder Markt- oder Meinungsforschung wird von den Bürgerinnen und Bürgern zunehmend als Belastung empfunden und ist mit dem Wunsch nach mehr Selbstbestimmung verbunden., dass eine verantwortliche Stelle ohne ihre Einwilligung ihre personenbezogenen Daten für fremde Werbezwecke gegen Entgelt an Dritte veräußern oder zur Anmietung zur Verfügung stellen darf. Zudem haben die öffentlich bekannt gewordenen Vorkommnisse deutlich gemacht, dass für eine effektivere Durchsetzung der bestehenden gesetzlichen Regelungen zum Datenschutz die Stellung der betrieblichen Beauftragten für den Datenschutz gestärkt werden muss und die Bußgeldtatbestände erweitert werden müssen, um zu einem wirksames Vorgehen der Aufsichtsbehörden beizutragen. Die vorgeschlagenen Änderungen resultieren in weiten Bereichen aus den Erfahrungen der Länder im Bereich der Aufsichtspraxis.

Das Datenschutzauditgesetz bietet Unternehmen die Möglichkeit, sich auf freiwilliger Basis einem Datenschutzaudit zu unterziehen und hierfür in ein Kontrollsystem einbeziehen zu lassen. Erfüllt ein Datenschutzkonzept oder eine technische Einrichtung von einem Datenschutzauditausschuss beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit festgelegte Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit und lassen die Unternehmen dies in einem formalisierten Verfahren durch Kontrollstellen regelmäßig überprüfen, können sie das Datenschutzkonzept oder die technische Einrichtung mit einem Datenschutzauditsiegel kennzeichnen. Auf diese Weise können Unternehmen einen Vorteil gegenüber Wettbewerbern erzielen, die sich keinem Datenschutzaudit unterziehen. Verbraucher können gekennzeichnete Datenschutzkonzepte oder technische Einrichtungen an dem Datenschutzauditsiegel erkennen und bei der Entscheidung zwischen mehreren Anbietern berücksichtigen. Anstrengungen, die über die gesetzlichen Anforderungen in Bezug auf den Datenschutz hinausgehen, können für Unternehmen einen wirtschaftlichen Mehrwert darstellen. Zugleich wird bei den Verbrauchern Bewusstsein für die Datenschutzrelevanz eines Produktes oder einer Dienstleistung geschaffen und gefördert.

II. Gesetzgebungskompetenz

Die Gesetzgebungskompetenz des Bundes folgt für Regelungen des Datenschutzes als Annex aus der Kompetenz für die geregelte Sachmaterie.

Betroffene Sachmaterien des Artikel 1 sind vorwiegend das Bürgerliche Recht (Artikel 74 Abs. 1 Nr. 1 Grundgesetz), das Recht der Wirtschaft (Artikel 74 Abs. 1 Nr. 11 Grundgesetz) und das Arbeitsrecht (Artikel 74 Abs. 1 Nr. 12 Grundgesetz). Die Berechtigung des Bundes zur Inanspruchnahme der Gesetzgebungskompetenz ergibt sich aus Artikel 72 Abs. 2 Grundgesetz. Eine bundeseinheitliche Regelung der gesetzlichen Erlaubnistatbestände für die Verarbeitung und Nutzung personenbezogener Daten zum Zwecke des Adresshandels und der Werbung, Markt- oder Meinungsforschung, des Kündigungsschutzes der Beauftragten für den Datenschutz und einer Informationspflicht von Unternehmen bei einer unbefugten Kenntniserlangung sensibler Daten durch Dritte ist zur Wahrung der Wirtschaftseinheit im Bundesgebiet im gesamtstaatlichen Interesse erforderlich. Eine unterschiedliche oder ausbleibende Regelung dieser Materien durch den Landesgesetzgeber würde zu erheblichen Nachteilen für die Gesamtwirtschaft führen, die sowohl im Interesse des Bundes als auch der Länder nicht hingenommen werden kann. Insbesondere wäre zu befürchten, dass unterschiedliche landesrechtliche Behandlungen gleicher Lebenssachverhalte erhebliche Wettbewerbsverzerrungen und störende Schranken für die länderübergreifende Wirtschaftstätigkeit zur Folge hätten. Bei unterschiedlichen Regelungen durch die Länder bestünde die Gefahr, dass einige Unternehmen weiterhin personenbezogene Daten ohne Einwilligung der Betroffenen zum Zwecke der Werbung, Markt- oder Meinungsforschung für Dritte verarbeiten und nutzen können, einen Beauftragten für den Datenschutz aus Gründen, die nicht auf sein Amt bezogen sind, kündigen können oder bei einer unbefugten Kenntniserlangung sensibler Daten durch Dritte die Aufsichtsbehörden und die Betroffenen nicht benachrichtigen müssen. Anderen Unternehmen in anderen Ländern bliebe diese Möglichkeit verwehrt bzw. sie wären zur Benachrichtigung verpflichtet, obwohl es sich um die gleichen personenbezogenen Daten handelt, die gleichen betrieblichen Voraussetzungen bestehen oder dieselbe unbefugte Kenntniserlangung sensibler Daten durch Dritte erfolgt ist. Es entstünden für letztere gravierende wettbewerbsverzerrende Änderungen, denen die erstgenannten Unternehmen nicht ausgesetzt wären. Zudem können die bestehenden Regelungen des Bundesdatenschutzgesetzes nur durch ein Bundesgesetz geändert werden.

Einem Datenschutzaudit nach Artikel 2 können sich private Unternehmen und diesen gleichgestellte öffentlich-rechtliche Wettbewerbsunternehmen unterziehen. Betroffene Sachmaterie ist daher ganz überwiegend das Recht der Wirtschaft (Artikel 74 Abs. 1 Nr. 11 Grundgesetz). Die Berechtigung des Bundes zur Inanspruchnahme der Gesetzgebungskompetenz ergibt sich aus Artikel 72 Abs. 2 Grundgesetz. Eine bundesgesetzliche Regelung über ein Datenschutzaudit ist zur Wahrung der Wirtschaftseinheit im Bundesgebiet im gesamtstaatlichen Interesse erforderlich. Eine unterschiedliche Regelung dieser Materie durch den Landesgesetzgeber oder sein Untätigbleiben würde zu erheblichen Nachteilen für die Gesamtwirtschaft führen, die sowohl im Interesse des Bundes als auch der Länder nicht hingenommen werden können. Insbesondere wäre zu befürchten, dass unterschiedliche landesrechtliche Behandlungen gleicher Lebenssachverhalte erhebliche Wettbewerbsverzerrungen und störende Schranken für die länderübergreifende Wirtschaftstätigkeit zur Folge hätten. Dies wäre etwa der Fall, wenn Datenschutzauditsiegel in den Ländern anhand unterschiedlicher Verfahren vergeben würden. Die landesrechtlich unterschiedliche Ausgestaltung des Kontrollverfahrens und des Verfahrens für die Zulassung der Kontrollstellen würde abweichende Maßstäbe bei der Prüfung und Bewertung nach sich ziehen. Unternehmen, die länderübergreifend oder bundesweit agieren, müssten sich für gleich bleibende Auditgegenstände unterschiedlichen Verfahren und Kontrollen durch wechselnde Personen unterziehen, mit der Gefahr abweichender Ergebnisse. In einem Land auditierte und mit einem Datenschutzauditsiegel gekennzeichnete Datenschutzkonzepte sowie technische Einrichtungen unterlägen in den einzelnen Ländern unterschiedlichen Bedingungen. Dies würde die Verwendbarkeit für die betroffenen Unternehmen nachhaltig beeinträchtigen. Unterschiedliche Landesregelungen zum Datenschutzauditverfahren würden zu einer gesamtstaatlich bedenklichen Verlagerung der wirtschaftlichen Aktivitäten in weniger kontrollintensive Länder führen. Unterläge ein Datenschutzkonzept oder eine technische Einrichtung in Länder verschärften Kontrollmaßnahmen, käme es unter Umständen dort nicht zum Einsatz. Dies hätte auch Folgen für Verb-

raucherinnen und Verbraucher, die in solchen Ländern auf auditierte Verfahren und Produkte nicht zurückgreifen könnten. Auch unterschiedliche Landesregelungen in Bezug auf den Kreis der in die Kontrollen einbezogenen Auditgegenstände bergen Gefahren für die Sicherheit und Verlässlichkeit des gesamten Kontrollverfahrens. Ein landesrechtlich unterschiedliches Kontrollniveau wäre den Verbraucherinnen und Verbrauchern auch nicht zu vermitteln. Das Vertrauen der Verbraucher in Datenschutzauditsiegel wäre insgesamt erschüttert. Auch für die Festlegung der von den Kontrollstellen zu erfüllenden Aufzeichnungs- und Meldepflichten ist eine bundesgesetzliche Regelung im gesamtstaatlichen Interesse notwendig. Im Falle landesrechtlich unterschiedlich geregelter Pflichten der Kontrollstellen bestünde die Gefahr, dass die für die Aufklärung von Verstößen wichtigen gegenseitigen Unterrichtungen, die gerade auch ein schnelles Tätigwerden der zuständigen Behörden ermöglichen sollen, ins Leere liefen. Nur durch eine bundesgesetzliche Regelung kann sichergestellt werden, dass für den Wirtschaftsstandort Deutschland einheitliche rechtliche Rahmenbedingungen im Hinblick auf die Verwendung des Datenschutzauditsiegels gegeben sind. Sinn des Datenschutzauditsiegels ist es gerade, durch seine einheitliche Ausgestaltung die Verbraucherinnen und Verbraucher über die zur Verbesserung des Datenschutzes beitragende Gestaltung zu informieren und hinsichtlich dieser Gestaltung für das gesamte Bundesgebiet einheitliche Standards zu setzen. Eine bundesgesetzliche Regelung ist ferner erforderlich, um einheitliche rechtliche Rahmenbedingungen im Hinblick auf den Schutz der Verbraucherinnen und Verbraucher durch Sanktionen bei Verstößen zu gewährleisten.

III. Vereinbarkeit mit dem Recht der Europäischen Union

Der Gesetzentwurf ist mit dem Recht der Europäischen Union vereinbar. Er steht insbesondere nicht im Widerspruch zu den Regelungen der Richtlinie 95/46/EG (EG-Datenschutzrichtlinie).

Die Stärkung der Unabhängigkeit des Beauftragten für den Datenschutz durch die Ermöglichung der Fortbildung fördert die Vorgabe in Artikel 18 Abs. 2 3. Spiegelstrich der Richtlinie. Danach sehen die Mitgliedstaaten eine „unabhängige Überwachung“ der Anwendung der zur Umsetzung der Richtlinie erlassenen einzelstaatlichen Bestimmungen durch den Beauftragten für den Datenschutz vor. Die Stärkung der Einwilligung und die Beschränkung der gesetzlichen Erlaubnis zur Verarbeitung und Nutzung personenbezogener Daten zu nicht ausschließlich eigenen Zwecken der Werbung, Markt- oder Meinungsforschung steht im Einklang mit den Regelungen der Richtlinie und wird insbesondere den aus Artikel 2 Buchstabe h, Artikel 7 Buchstabe a und Artikel 14 Satz 1 Buchstabe b der Richtlinie abzuleitenden Zielen gerecht.

Bei einem Datenschutzaudit nach dem Gesetzentwurf werden Datenschutzkonzepte oder technische Einrichtungen anhand von Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit überprüft, die über die Vorschriften hinausgehen, die die Vorgaben der EG-Datenschutzrichtlinie Der Gesetzentwurf fördert daher mittelbar die tatsächliche Durchsetzung dieser Regelungen.

IV. Finanzielle Auswirkungen auf die öffentlichen Haushalte

Das Gesetz bewirkt keine Haushaltsausgaben ohne Vollzugsaufwand.

In Bezug auf das Datenschutzauditgesetz entsteht bei den zuständigen Behörden der Länder Vollzugsaufwand. Sie haben die zugelassenen Kontrollstellen, die das Kontrollverfahren durchführen, zu überwachen und Verstöße dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit mitzuteilen. Bestimmte hoheitliche Maßnahmen sind ihnen vorbehalten. Die Kosten für die einzelnen Amtshandlungen der zuständigen

Behörden können vom Bund und den Ländern durch Kostenordnungen auf die Antragsteller abgewälzt werden.

Vollzugsaufwand entsteht durch die Bildung eines Datenschutzauditausschusses mit Vertretern aus Bund, Ländern und der Wirtschaft nebst Geschäftsstelle beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Die Tätigkeit der Vertreter erfolgt ehrenamtlich.

Weiterer Vollzugsaufwand entsteht beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit in einem Teilbereich durch die Überwachung der Kontrollstellen. Ferner durch die Zulassung und die Entziehung der Zulassung gegenüber den Kontrollstellen und die Führung eines Registers der angezeigten Datenschutzkonzepte und technischen Einrichtungen sowie der zugelassenen Kontrollstellen.

Für den Vollzugsaufwand beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit werden in Abhängigkeit von der Zahl der Kontrollstellen zusätzliche Stellen sowie jährlich Haushaltsmittel für Personal- und Sachausgaben benötigt. Eine Kompensation aus dem Einzelplan 06 ist nicht möglich. Über die Ausbringung und Finanzierung dieser Personal- und Sachausgaben ist im Haushaltsaufstellungsverfahren 2009 zu entscheiden.

IV. Kosten

Kosten für die Wirtschaft entstehen, soweit nach Ablauf der Übergangsvorschrift künftig eine Einwilligung der Betroffenen einzuholen ist, um deren personenbezogene Daten für Zwecke der Werbung, Markt- oder Meinungsforschung zu verarbeiten und nutzen. Ferner können Kosten für die Wirtschaft entstehen, soweit diese künftig verpflichtet sind, bei unrechtmäßiger Kenntniserlangung bestimmter Daten durch Dritte die Aufsichtsbehörden und die Betroffenen bzw. ersatzweise die Öffentlichkeit zu benachrichtigen.

Kosten für die Wirtschaft können nach Maßgabe von ggf. von den Ländern und dem Bund zu erlassenden Kostenordnungen entstehen, durch die die Kosten für die einzelnen Auditverfahren auf die Antragsteller abgewälzt werden können. Des Weiteren wird die Durchführung des Audits (Sammeln und Zuverfügungstellen von Informationen, ggf. erforderliche Nachbesserungen am Gegenstand des Audits) Kosten bei den kontrollierten Stellen verursachen. Die Höhe dieser Kosten lässt sich zum gegenwärtigen Zeitpunkt nicht näher beziffern, da die konkrete Ausgestaltung des Verfahrens einer noch zu erlassenden Rechtsverordnung vorbehalten ist und die Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit als Maßstab der Prüfung von einem noch zu errichtenden Datenschutzauditausschuss zu beschließen sind. Kosten entstehen bei den Stellen, die sich beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu Kontrollstellen zulassen und im Rahmen des Kontrollsystems gegen angemessene Vergütung Kontrollen durchführen und dabei von den zuständigen Behörden der Länder überwacht werden.

Zusätzliche Kosten für Bürgerinnen und Bürger sind nicht zu erwarten.

Zusätzliche Kosten für die Verwaltung entstehen nicht. Auswirkungen auf Einzelpreise und das allgemeine Preisniveau, insbesondere auf das Verbraucherpreisniveau, sind nicht zu erwarten.

V. Bürokratiekosten[1]

Der vorliegende Gesetzentwurf enthält fünfzehn neue Informationspflichten für die Wirtschaft.

Der geplante § 44a des Bundesdatenschutzgesetzes verpflichtet nicht-öffentliche Stellen die Aufsichtsbehörde und die Betroffenen unverzüglich zu benachrichtigen, wenn bestimmte sensible Daten unrechtmäßig Dritten zur Kenntnis gelangt sind. Soweit die Benachrichtigung der Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, insbesondere aufgrund der Vielzahl der betroffenen Fälle, tritt an ihre Stelle die Information an die Öffentlichkeit durch Anzeigen, die mindestens eine halbe Druckseite umfassen, in mindestens zwei bundesweit erscheinenden Tageszeitungen.

Das Datenschutzauditgesetz enthält für die Wirtschaft folgende neue Informationspflichten:

Eine Kontrollstelle hat ihre Zulassung zu beantragen (§ 4 Abs. 1) und kann diese auf einzelne Länder beschränken (§ 4 Abs. 2 Satz 2). Auf Antrag der Kontrollstelle kann ihr eine Ausnahme von der Einbeziehung von einem Datenschutzkonzept oder einer technischen Einrichtungen in ihre Kontrollen gewährt werden (§ 5 Abs. 1 Satz 2). Jährlich hat die Kontrollstelle den zuständigen Behörden ein Verzeichnis der nicht-öffentlichen Stellen, die am 31. Dezember des Vorjahres ihrer Kontrolle unterstanden und bis spätestens zum 31. März jedes Jahres einen Bericht über ihre Tätigkeit im Vorjahr vorzulegen (§ 5 Abs. 2). Die Kontrollstellen erteilen einander die für eine ordnungsgemäße Durchführung dieses Gesetzes notwendigen Auskünfte (§ 5 Abs. 3 Satz 1). Stellt eine Kontrollstelle Unregelmäßigkeiten oder Verstöße fest, unterrichtet sie unverzüglich die zuständige Behörde bzw. im Rahmen des § 2 Abs. 1 Satz 2 den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (§ 5 Abs. 3 Satz 2). Soweit eine Kontrollstelle im Rahmen der von ihr durchgeführten Kontrollen Tatsachen feststellt, die einen hinreichenden Verdacht auf Unregelmäßigkeiten oder Verstöße der in Satz 2 genannten Art begründen, der eine nicht von der Kontrollstelle kontrollierte nicht-öffentliche Stelle betrifft, teilt die Kontrollstelle die Tatsachen unverzüglich der Kontrollstelle mit, deren Kontrolle die betroffene nicht-öffentliche Stelle untersteht (§ 5 Abs. 3 Satz 3). Die Kontrollstelle unterrichtet die von ihr kontrollierten nicht-öffentlichen Stellen, die zuständigen Behörden sowie den Bundesbeauftragten für den Datenschutz und Informationsfreiheit bevor sie ihre Tätigkeit einstellt oder im Falle eines Antrags auf Eröffnung des Insolvenzverfahrens (§ 5 Abs. 4 Satz 1). Nicht-öffentliche Stellen sowie Kontrollstellen haben den zuständigen Behörden auf Verlangen Auskünfte zu erteilen (7 Abs. 1). Auf ihr Aussageverweigerungsrecht sind sie hinzuweisen (§ 7 Abs. 4 Satz 2). Vor der erstmaligen Verwendung des Datenschutzauditsiegels ist das Datenschutzkonzept oder die technische Einrichtung dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit anzuzeigen (§ 8 Abs. 2 Satz 1). Abweichend von § 44a des Bundesdatenschutzgesetzes haben nicht-öffentliche Stellen die unbefugte Kenntniserlangung unverzüglich der zuständigen Kontrollstelle mitzuteilen (§ 19).

Die für die Wirtschaft entstehenden Kosten sind hinnehmbar, weil das Datenschutzaudit freiwillig ist und es die Unternehmen daher von einer Wirtschaftlichkeitsbetrachtung abhängig machen können, ob sie sich einem Audit mit den damit ggf. einhergehenden Bürokratiekosten unterziehen. Sofern ein Unternehmen sich entscheidet, als Kontrollstelle gegen Kontrollen durchzuführen, erfolgt dies gegen angemessene Vergütung. Die durch die Benennung der Vertreter für den Datenschutzauditausschuss und das Erzielen eines Einvernehmens über deren Person verursachten Kosten fallen nicht ins Gewicht und werden

[1] Die Abschätzung und Ausweisung der Bürokratiekosten erfolgt im Zuge der Ressortabstimmung und wird bis spätestens zum Ende der Ressortabstimmung in dem Entwurf ergänzt.

durch die Mitwirkung an der Erarbeitung des Prüfmaßstabs des Datenschutzauditverfahrens aufgewogen.

Für Bürgerinnen und Bürger wird eine neue Informationspflicht eingeführt. Die Verarbeitung und Nutzung ihrer personenbezogenen Daten durch die erhebende verantwortliche Stelle für nicht ausschließlich eigene Angebote betreffende Werbung oder eigene Markt- oder Meinungsforschung bedarf künftig ihrer schriftlichen Einwilligung. Auswirkungen auf Einzelpreise und das allgemeine Preisniveau, insbesondere auf das Verbraucherpreisniveau, sind nicht zu erwarten.

Für die Verwaltung enthält das Datenschutzauditgesetz zwölf neue Informationspflichten:

Für die Länder entstehen folgende neue Informationspflichten: Die zuständigen Behörden erteilen einander die zur Überwachung der Kontrollstellen notwendigen Auskünfte (§ 6 Abs. 1 Satz 2) und regen direkt oder über die zuständige Behörde des Landes, in dem der Sitz oder die Niederlassung der Kontrollstelle liegt, beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit die Entziehung der Zulassung oder die Aufnahme oder Änderung von Auflagen an (§ 6 Abs. 1 Satz 3 Nr. 1, 2, Satz 4). Zudem haben sie Auskunftspflichtige auf ihr Auskunftsverweigerungsrecht hinzuweisen (§ 7 Abs. 4 Satz 2).

Für den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit enthält das Gesetz folgende neue Informationspflichten: Er führt ein Verzeichnis der von ihm zugelassenen Kontrollstellen und der ihm angezeigten Datenschutzkonzepte und technischen Einrichtungen und veröffentlicht dies im elektronischen Bundesanzeiger und im Internet (§ 8 Abs. 2 Satz 2 und 3 Satz 1). In Bezug auf den bei ihm errichteten Datenschutzauditausschuss hat der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit die vom Ausschuss erlassenen Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit zu veröffentlichen (§ 11 Abs. 1 Satz 3) Der Datenschutzauditausschuss als Gremium muss im Rahmen der Rechtsaufsicht auf Verlangen der Aufsichtsbehörde Berichte und Akten vorlegen (§ 15 Abs. 2 Satz 3) und seine Beschlüsse bedürfen der Genehmigung durch die Aufsichtsbehörde (§ 15 Abs. 3 Satz 1).

Die Informationspflichten für die Verwaltung sind für die sinnvolle Gestaltung des Datenschutzauditverfahrens unerlässlich. Sie sind auch hinnehmbar, weil die Stärkung des Datenschutzes und die Förderung der Wirtschaft, die das Gesetz bewirkt, den nachteiligen Effekt der Bürokratiekosten überwiegen.

VI. Auswirkungen von gleichstellungspolitischer Bedeutung

Auswirkungen von gleichstellungspolitischer Bedeutung sind nicht zu erwarten.

B. Besonderer Teil

Zu Artikel 1

Zu Nummer 1 (Inhaltsübersicht):

Die Inhaltsübersicht ist an die nachfolgend begründeten Gesetzesänderungen anzupassen.

Zu Nummer 2 (§ 4f Abs. 3 Satz 5)

Durch die Änderung soll die Position des Beauftragten für den Datenschutz gestärkt werden. Satz 5 unterstützt die Fortbildung und damit die fachliche Eignung des Beauftragten für den Datenschutz.

Satz 5 sieht vor, dass die verantwortliche Stelle dem Beauftragten für den Datenschutz ermöglichen muss, an Schulungs- und Bildungsveranstaltungen teilzunehmen. Zugleich wird die verantwortliche Stelle verpflichtet, die Kosten hierfür zu übernehmen. Die Reichweite der Vorschrift, z.B. der Umfang und die thematische Ausrichtung der Fortbildung richtet sich nach der erforderlichen Fachkunde des Beauftragten für den Datenschutz, die er zur Erfüllung seiner Aufgaben benötigt. Insoweit ist § 4f Abs. 2 Satz 2 zu beachten. Danach richtet sich das Maß der erforderlichen Fachkunde insbesondere nach dem Umfang der Datenverarbeitung und dem Schutzbedarf der personenbezogenen Daten, die die verantwortliche Stelle erhebt oder verwendet. Der Fortbildungsbedarf der Beauftragten für den Datenschutz variiert daher jenseits eines Grundbedarfs, der auch durch die stetige Fortentwicklung von Recht und Technik hervorgerufen wird. Ähnliche Regelungen bestehen z.B. für Betriebs- und Personalräte (§ 37 Abs. 6 Satz 1 des Betriebsverfassungsgesetzes, § 46 Abs. 6 des Bundespersonalvertretungsgesetzes).

Zu Nummer 3 (§ 9a)

Der bisherige § 9a sieht die Möglichkeit eines Datenschutzaudits vor und kündigt in Satz 2 ein ausführendes Gesetz hierzu an. Dieses ist in Art. 2 vorgesehen. Die Aufhebung des bisherigen § 9a ist daher eine notwendige Folgeänderung.

Zu Nummer 4 (§ 12 Abs. 4)

Die Änderung in Absatz 4 ist eine redaktionelle Anpassung an die Verschiebung des Erlaubnistatbestandes des bisherigen Absatzes 3 Satz 1 Nr. 1 zum geplanten Absatz 2 Nr. 2 Buchstabe a.

Zu Nummer 5 (§ 28)

Die vorgeschlagene Regelung beinhaltet die Streichung des bisher in § 28 Abs. 3 Satz 1 Nr. 3 geregelten, sog. „Listenprivilegs“ und die Einführung eines begrenzten Kopplungs-

verbots für marktbeherrschende Unternehmen im neuen Absatz 3b. Die weiteren Änderungen sind redaktionelle Änderungen und Folgeänderungen.

Der bisherige § 28 Abs. 2 und Abs. 3 sind ohne inhaltliche Änderung zusammengeführt worden. Beide enthielten gesetzliche Erlaubnistatbestände zur Übermittlung und Nutzung personenbezogener Daten zu einem anderen Zweck. Dies kam bislang in § 28 Abs. 3 Satz 1 durch das Wort „auch“ zum Ausdruck. Der bisherige Absatz 2 ist nunmehr Absatz 3 Nr. 1. Die bisherigen Erlaubnistatbestände in Absatz 3 Satz 1 Nr. 1 und 2 sind sprachlich zusammengefasst worden und nunmehr Absatz 3 Nr. 2 Buchstabe a und b. Die bisherige Absatz 3 Satz 1 Nr. 4 ist nunmehr Absatz 3 Nr. 3.

Der bisherige § 28 Abs. 3 Satz 1 Nr. 3, das sog. „Listenprivileg“ wurde gestrichen. Der bisherige § 28 Abs. 3 Satz 2 wurde infolge der geplanten Neuregelung in § 28 Abs. 3 entbehrlich. Auch nach der Streichung des § 28 Abs. 3 Satz 1 Nr. 3 bleibt eine Übermittlung und Nutzung für Zwecke der Werbung oder Markt- oder Meinungsforschung nach dem Erlaubnistatbestand in § 28 Abs. 1 Satz 1 Nr. 2 zulässig, d.h. die Übermittlung eigener Datenbestände zur Erfüllung eigener Geschäftszwecke an Dritte und die Nutzung eigener Datenbestände, um zur Erfüllung eigener Geschäftszwecken für Dritte z.B. zu werben. Da § 28 Abs. 1 Satz 1 Nr. 2 eine Abwägung der berechtigten Interessen der verantwortlichen Stelle mit den schutzwürdigen Interessen des Betroffenen vorsieht, würde dies den Betroffenen effektiv schlechter stellen, weil der bisherige § 28 Abs. 3 Satz 1 Nr. 3 allein das Bestehen schutzwürdiger Interessen des Betroffenen genügen lässt.

Der vorgesehene Absatz 3 sieht daher vor, dass bei der Verarbeitung oder Nutzung personenbezogener Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung anzunehmen ist, dass das schutzwürdige Interesse des Betroffenen überwiegt und mit Ausnahme der nachfolgend geregelten Nummern 1, 2 und 3 grundsätzlich nicht zulässig ist.

Die erste Ausnahme in dem geplanten § 28 Abs. 3 Nr. 1 sieht vor, dass nicht anzunehmen ist, dass das schutzwürdige Interesse überwiegt, wenn die Verarbeitung oder Nutzung ausschließlich für Zwecke der Werbung für eigene Angebote oder der eigenen Markt- oder Meinungsforschung der verantwortlichen Stelle erfolgen soll, die die Daten von dem Betroffenen nach § 28 Abs. 1 Satz 1 Nr. 1 erhoben hat. Die Formulierung orientiert sich dabei an der bereichsspezifischen Regelung des § 95 Abs. 2 Satz 1 des Telekommunikationsgesetzes zur Verwendung von Telekommunikationsbestandsdaten durch die Dienstanbieter. Ein überwiegendes schutzwürdiges Interesse des Betroffenen ist insofern nicht kraft Gesetzes anzunehmen, weil dem Betroffenen die verantwortliche Stelle durch die Erhebung der Daten im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Verhältnisses bekannt ist und er auch damit rechnen kann, dass ihn die verantwortliche Stelle Werbung für weitere eigene Angebote der verantwortlichen Stelle zukommen lässt oder im Interesse der Fortsetzung des bestehenden Vertrags- oder vertragsähnlichen Verhältnisses eigene Markt- oder Meinungsforschung betreibt. Insoweit ist es ausreichend, dass der Betroffene gegenüber der ihm auch bekannten verantwortlichen Stelle Gebrauch von seinem Widerspruchsrecht nach § 28 Abs. 4 Satz 1 machen kann. Eine Kennzeichnung der Daten, um deren Herkunft nachvollziehen zu können, ist in dieser Konstellation damit auch entbehrlich.

Nicht erfasst von dem geplanten § 28 Abs. 3 Nr. 1 ist hingegen die Verarbeitung oder Nutzung die nicht der eigenen Markt- oder Meinungsforschung oder Zwecken der Werbung dient, die nicht ausschließlich eigenen Angebote betreffen. Insoweit rechnet der Betroffene nicht damit, dass die verantwortliche Stelle seine personenbezogenen Daten, die sie im Rahmen eines Vertrags- oder vertragsähnlichen Verhältnisses erhoben hat, ohne weiteres Zutun des Betroffenen auch dazu verwendet, sie an weitere Dritte zu veräußern oder diesen zur Verfügung zu stellen, damit diese an den Betroffenen mit ihren Angeboten herantreten.

Die zweite Ausnahme in dem geplanten § 28 Abs. 3 Nr. 2 sieht daher vor, dass nicht anzunehmen ist, dass das schutzwürdige Interesse des Betroffenen überwiegt, wenn dieser in die Verarbeitung oder Nutzung eingewilligt hat, wobei die Einwilligung den besonderen Vorgaben des Absatzes 3a unterworfen wird und durch Verweis Absatz 3b zu beachten ist. Die verantwortliche Stelle muss daher in Zukunft an den Betroffenen herantreten und ihn, z.B. durch die Gewährung von Vorteilen, für eine Einwilligung gewinnen. Diese in einigen Wirtschaftsbereichen schon übliche Praxis, z.B. im Rahmen von Kundenbindungsprogrammen durch Gewährung von Vorteilen (ggf. gewisser zusätzlicher Punktwerte) eine Gegenleistung des Kunden in Form einer Einwilligung zu erhalten, wird zu auf Einwilligung gegründeten kommerziellen Datenbeständen führen. Eine gesetzliche Kennzeichnungspflicht der Daten, um deren Herkunft nachvollziehen zu können, ist auch in dieser Konstellation nicht erforderlich. Da die Zulässigkeit der Datenverarbeitung auf der Einwilligung des Betroffenen beruht, ist diese von den verantwortlichen Stellen gegenüber ihren Vertragspartnern aber auch bei aufsichtsbehördlichen Kontrollen nachzuweisen. Die konkrete Umsetzung bleibt der Wirtschaft überlassen, wird aber mit gewissen Kosten verbunden sein.

Die dritte Ausnahme in dem geplanten § 28 Abs. 3 Nr. 3 sieht vor, dass nicht anzunehmen ist, dass das schutzwürdige Interesse des Betroffenen überwiegt, wenn die Verarbeitung oder Nutzung für Zwecke der Spendenwerbung einer verantwortlichen Stelle erfolgen soll, die ausschließlich und unmittelbar steuerbegünstigte Zwecke nach § 51 der Abgabenordnung verfolgt und wenn es sich um die in dem bisherigen § 28 Abs. 3 Satz 1 Nr. 3 genannten „Listendaten“ handelt. Insofern wird der bestehende Zustand beibehalten. Zu den steuerbegünstigten Zwecken gehören gemeinnützige, mildtätige und kirchliche Zwecke nach den §§ 52 bis 54 der Abgabenordnung. Die verantwortliche Stelle muss diese Zwecke ausschließlich und unmittelbar verfolgen (§§ 56, 57 der Abgabenordnung). Die Ausnahme ist beschränkt auf die Verarbeitung und Nutzung der Daten für Zwecke der Spendenwerbung. Die Regelung begünstigt, in Anlehnung an bestehende steuerliche Vergünstigungen, den finanziellen Fortbestand der Organisationen, in dem die werbliche Ansprache von Spendern erleichtert wird. Auch insoweit ist es ausreichend, dass der Betroffene Gebrauch von seinem Widerspruchsrecht nach § 28 Abs. 4 Satz 1 machen kann. Im Hinblick auf das öffentliche Interesse, das an Spenden an steuerbegünstigte Organisationen einerseits besteht und den erheblichen Aufwand, den eine Kennzeichnung andererseits mit sich bringen würde, ist insoweit eine Pflicht zur Kennzeichnung der Herkunft der Daten verzichtbar.

Nach dem geplanten Absatz 3a Satz 1 bedarf die Einwilligung der Schriftform. Abweichend von § 4a Abs. 1 Satz 3, der wegen besonderer Umstände auch eine andere Form erlaubt, soll die Schriftform vorliegend ohne Zweifel dokumentieren, dass der Betroffene sich mit seiner Willensbekundung einverstanden hat, dass seine personenbezogenen Daten auch für fremde Zwecke der Werbung oder Markt- oder Meinungsforschung übermittelt oder genutzt werden können. Die Schriftform soll dabei ermöglichen, etwaige Grenzen der Einwilligung, z.B. nur innerhalb des Konzerns oder nur an bestimmte Dritte oder nur Nutzung aber keine Übermittlung, nachzuvollziehen. Zugleich soll die Schriftform den Betroffenen die Bedeutung der Einwilligung vor Augen führen, da die hierdurch ermöglichte Übermittlung an Dritte es ihm künftig erschwert, von seinem Widerspruchsrecht nach § 28 Abs. 4 Satz 1 Gebrauch zu machen. Nach dem geplanten Satz 2 kann die Einwilligung auch elektronisch erklärt werden, wenn die verantwortliche Stelle bestimmte technische Vorkehrungen trifft, die sich in dieser Form bereits in § 94 des Telekommunikationsgesetzes und § 13 Abs. 2 des Telemediengesetzes wieder finden. Die verantwortliche Stelle hat bei einer elektronisch erklärten Einwilligung sicherzustellen, dass die Einwilligung protokolliert wird und der Betroffene den Inhalt der Einwilligung jederzeit abrufen und die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann. Satz 2 enthält keine, insbesondere keine von § 126a des Bürgerlichen Gesetzbuches abweichenden, Vorgaben zur elektronischen Form der Erklärung. Der geplante Satz 3 sieht vor, dass die Einwilligung, wenn sie im Zusammenhang mit anderen Erklärungen erteilt wird, nur wirksam ist, wenn der Betroffene durch Ankreuzen, durch eine gesonderte Unterschrift oder

ein anderes, ausschließlich auf die Einwilligung in die Weitergabe seiner Daten für Werbezwecke bezogenes Tun zweifelsfrei zum Ausdruck bringt, dass er die Einwilligung bewusst erteilt. § 4a Abs. 1 Satz 4 sieht insoweit lediglich vor, dass die Einwilligung besonders hervorgehoben werden muss, z.B. durch Schriftgröße und Gestaltung. Der geplante Satz 3 will für den hier zu regelnden Bereich sicherstellen, dass es keinen Zweifel darüber gibt, dass der Betroffene seine Einwilligung in die Weitergabe seiner Daten für Werbezwecke gegeben hat.

Der geplante Absatz 3b sieht vor, dass die verantwortliche Stelle sich die Einwilligung des Betroffenen in eine Verarbeitung oder Nutzung seiner personenbezogenen Daten, die nicht ausschließlich Zwecken der Werbung für eigene Angebote oder der eigenen Markt- oder Meinungsforschung dient, nicht auf dem Wege verschaffen darf, dass sie hiervon den Abschluss eines Vertrages abhängig macht. Dieses Kopplungsverbot von Vertragsabschluss und Einwilligung ist aufgrund seiner Einschränkung der Vertragsgestaltungsfreiheit auf die Fälle begrenzt, in denen dem Betroffenen ein anderer Zugang zu der vertraglichen Gegenleistung ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist. Die Formulierung lehnt sich damit an die bestehenden bereichsspezifischen Kopplungsverbote im § 95 Abs. 5 des Telekommunikationsgesetzes und in § 12 Abs. 3 des Telemediengesetzes an.

Die vorgesehenen Änderungen in Absatz 4 sind redaktionelle Anpassungen an die Formulierung des geplanten Absatzes 3.

Die Änderung in Absatz 9 Satz 4 ist eine redaktionelle Anpassung an die Verschiebung des Erlaubnistatbestandes des bisherigen Absatzes 3 Satz 1 Nr. 2 zum geplanten Absatz 2 Nr. 2 Buchstabe b.

Zu Nummer 6 (§ 29)

Die Änderungen in § 29 Abs. 1 und 2 sind notwendige redaktionelle Änderungen und Folgeänderungen durch die die Änderungen in § 28 Abs. 3 bis 3b auch auf die geschäftsmäßige Datenerhebung und -verarbeitung übertragen werden.

Die Änderungen in Absatz 1 Satz 1 sind redaktionelle Anpassungen an § 28. Die Vorschrift in Absatz 1 Satz 2 sieht vor, dass die Änderungen in § 28 Abs. 3 bis 3b auch für die geschäftsmäßige Erhebung, Speicherung oder Veränderung personenbezogener Daten zum Zweck der Übermittlung gelten.

Die Änderungen in Absatz 2 Satz 1 sind redaktionelle Folgeänderungen aus der Streichung des § 28 Abs. 3 Satz 1 Nr. 3. Die Vorschrift in Absatz 2 Satz 2 sieht vor, dass die Änderungen in § 28 Abs. 3 bis 3b auch für die geschäftsmäßige Übermittlung im Rahmen der Zwecke nach § 29 Abs. 1 gelten.

Zu Nummer 7 (§ 33 Abs. 2 Satz 1 Nr. 8 Buchstabe b)

Es handelt sich um eine Folgeänderung der unter Ziffer 5 vorgesehenen Änderung. Bislang bestand keine Pflicht zur Benachrichtigung, wenn die Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert sind und es sich um listenmäßig oder sonst zusammengefasste Daten handelte und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist. Mit der Streichung dieser Regelung im bisherigen § 29 Abs. 2 Nr. 1 Buchstabe b entfällt auch die Ausnahme von der Benachrichtigungspflicht.

Zu Nummer 8 (§ 43)

Die Änderungen in § 43 zielen auf eine Erweiterung des Bußgeldtatbestandes, indem eine Lücke bei den Bußgeldtatbeständen geschlossen wird und der bestehende Bußgeldrahmen erhöht sowie die ausdrückliche Möglichkeit eingeräumt wird, bei der Bußgeldbemessung den wirtschaftlichen Vorteil des Täters aus der Ordnungswidrigkeit zu übersteigen.

Derzeit ist nach § 43 Abs. 2 Nr. 1 die unbefugte Erhebung oder Verarbeitung personenbezogener Daten, die nicht allgemein zugänglich sind bußgeldbewehrt, die unbefugte Nutzung hingegen nicht. Dies führt zu Wertungswidersprüchen. Eine verantwortliche Stelle, die personenbezogene Daten unbefugt erhebt und speichert kann hierfür belangt werden, nicht jedoch für eine unbefugte Auswertung oder einen sonstigen zielgerichteten Gebrauch, obwohl dieser den Verstoß vertieft. Daher ist künftig vorgesehen, auch für die unbefugte Nutzung personenbezogener Daten die Möglichkeit einer Bußgeldbewehrung vorzusehen.

Der derzeitige Bußgeldrahmen für Verstöße gegen den Bußgeldkatalog des § 43 Abs. 1 beträgt 25.000 EUR, für Verstöße gegen den Bußgeldkatalog des § 43 Abs. 2 beträgt er 250.000 EUR. Der Bußgeldrahmen geht zurück auf die Überarbeitung der Straf- und Bußgeldvorschriften im Jahre 2001. Seit dem hat sich die Informationstechnik weiter verbreitet und durchdringt zunehmend auch wirtschaftlich relevante Bereiche des alltäglichen Lebens. Damit einher geht eine wachsende wirtschaftlich Bedeutung personenbezogener Daten und ein gesteigertes Missbrauchspotential, das mittlerweile geschäftsmäßig genutzt wird. Der Abschreckungseffekt des bisherigen Bußgeldrahmens ist dadurch erodiert, was sich u. a. in einer gestiegenen Zahl öffentlich bekannt gewordener Verstöße niederschlägt. Die gestiegene, auch wirtschaftliche Bedeutung des Datenschutzrechts spiegelt sich nicht mehr ausreichend in dem bestehenden Bußgeldrahmen wider, der hinter jüngeren, vergleichbaren Bußgeldrahmen des bereichsspezifischen Datenschutzrechts zurückbleibt. So sieht der Bußgeldrahmen im Bereich des Telekommunikationsrechts in § 149 Abs. 2 des Telekommunikationsgesetzes und auch der Bußgeldrahmen des Entwurfs für ein Gendiagnostikgesetz in § 26 Abs. 2 einen Bußgeldrahmen von 300.000 EUR vor. Der Bußgeldrahmen für Verstöße gegen materielle Vorschriften im Bußgeldkatalog des § 43 Abs. 2 ist daher moderat von 250.000 EUR auf 300.000 EUR anzupassen. Zugleich wird der Bußgeldrahmen für Verstöße gegen Verfahrensvorschriften im Bußgeldkatalog des § 43 Abs. 1 von 25.000 EUR auf 50.000 EUR erhöht. Dadurch soll auch der relativ gestiegenen Bedeutung der Verfahrensvorschriften,, wie etwa die Meldepflicht automatisierter Verarbeitungen gegenüber den Aufsichtsbehörden oder die Pflicht zur Bestellung eines Beauftragten für den Datenschutz, gegenüber den materiellen Schutzvorschriften Rechnung getragen werden.

Die neuen Sätze 2 und 3 treten ergänzend zu der Verschärfung des Bußgeldrahmens. Sie stellen sicher, dass dem Täter aus der Ordnungswidrigkeit kein wirtschaftlicher Vorteil verbleibt und einen Anreiz für weitere Verstöße bietet. Satz 2 sieht insoweit als Vorgabe für die Bemessung der Geldbuße vor, dass sie den wirtschaftlichen Vorteil übersteigen soll. Soweit hierfür im Einzelfall auch der nun erhöhte Bußgeldrahmen nicht ausreicht, kann er überschritten werden. Die Regelungen sollen in Anlehnung an bereichsspezifische Vorbilder, z.B. in § 149 Abs. 3 Satz 2, 3 des Telekommunikationsgesetzes oder § 81 Abs. 5 des Gesetzes gegen Wettbewerbsbeschränkungen, eine Hervorhebung und Klarstellung für die Aufsichtsbehörden in der Vollzugspraxis mit sich bringen, die in der Vergangenheit aufgrund rechtlicher oder tatsächlicher Zweifel von der Möglichkeit keinen Gebrauch gemacht haben.

Zu Nummer 9 (§ 44a)

Die Vorschrift enthält eine Informationspflicht für nicht-öffentliche Stellen und ihnen gleichgestellte Wettbewerbsunternehmen, öffentliche Stellen wurden aufgrund des Gleichklangs mit auditierten Unternehmen aus systematischen Gründen nicht einbezogen. Die Informationspflicht besteht, wenn bestimmte besonders sensible personenbezogene Daten aus dem Verfügungsbereich der Informationsverpflichteten Dritten unrechtmäßig zur Kenntnis gelangen und dadurch schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen. Letzteres bestimmt sich unter anderem nach der Art der betroffenen Daten, und den potenziellen Auswirkungen der unrechtmäßigen Kenntniserlangung durch Dritte auf die Betroffenen (z.B. materielle Schäden bei Kreditkarteninformationen oder soziale Nachteile einschließlich des Identitätsbetrugs). Die Vorschrift knüpft an einen Vorschlag der Kommission der Europäischean Gemeinschaften zur Änderung der Richtlinie 2202/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (KOM(2007) 698 endg.) und Regelungen im Recht der Vereinigten Staaten von Amerika an. Die Informationspflicht ist auf besonders sensible personenbezogene Daten aus dem Verfügungsbereich der verantwortlichen Stelle begrenzt. Hierzu gehören besondere Arten personenbezogener Daten nach § 3 Abs. 9, personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten beziehen, Daten zu Bank- oder Kreditkartenkonten und Bestandsdaten nach § 3 Nr. 3 des Telekommunikationsgesetzes sowie Verkehrsdaten nach § 3 Nr. 30 des Telekommunikationsgesetzes sowie Bestandsdaten nach § 14 des Telemediengesetzes und Nutzungsdaten nach § 15 des Telemediengesetzes. Voraussetzung ist, dass die verantwortliche Stelle anhand von tatsächlichen Anhaltspunkten, z.B. aus dem eigenen Sicherheitsmanagement oder durch Hinweise von Strafverfolgungsorganen und unter Einbeziehung des Beauftragten für den Datenschutz nach § 4g Abs. 1 Satz 1 feststellt, dass personenbezogene Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten nach § 3 Abs. 8 Satz 2 zur Kenntnis gelangt sind. Die verantwortliche Stelle hat – unter Einbeziehung des Beauftragten für den Datenschutz nach § 4g Abs. 1 Satz 1 – in diesem Fall sowohl die zuständige Datenschutzaufsichtsbehörde als auch die Betroffenen zu informieren. Bei nicht-öffentlichen Stellen ist die zuständige Datenschutzaufsichtsbehörde grundsätzlich die Aufsichtsbehörde nach § 38, bei Post- und Telekommunikationsunternehmen der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit nach § 24. Die Benachrichtigung soll unverzüglich, d.h. nach der Legaldefinition des § 121 des Bürgerlichen Gesetzbuches ohne schuldhaftes Zögern - ergehen. § 44a stellt im 2. Halbsatz klar, dass ein schuldhaftes Zögern insbesondere dann nicht gegeben ist, soweit die Datensicherungspflichten des § 9 oder Interessen der Strafverfolgung einer Veröffentlichung der Datenschutzverletzung vorläufig noch entgegenstehen. Im ersteren Fall zielt die Regelung darauf ab, dem Verpflichteten die Möglichkeit zu geben, etwaige technische Sicherheitslücken, unter deren Ausnutzung die Datenschutzverletzung erfolgte, zu analysieren und so weit wie möglich zu beheben, bevor breitere Kreise von der Lücke Kenntnis erhalten. Andernfalls besteht Gefahr, dass Dritte von dieser Kenntnis profitieren, um selbst die fragliche Sicherheitslücke auszunutzen. Dies entspricht dem in Fachkreisen mit "Responsible Disclosure" ("Verantwortungsvolle Offenlegung") bezeichneten Vorgehen. Nach den Grundsätzen der "Responsible Disclosure" wird nach dem Finden einer Schwachstelle als erstes der Hersteller informiert. Erst nach einer angemessenen Frist wird die Schwachstelle und die diese ausnutzende Software veröffentlicht. Der Hersteller soll damit die Möglichkeit bekommen, das Problem zu beheben, indem er eine neue, sichere Version seiner Software erstellt. Auch soll der Hersteller dadurch in der Lage versetzt werden, die Anwender über die neue Version der Software zu informieren und sie an die Anwender zeitnah auszuliefern. Im zweiten Fall dürfen Ermittlungen der Strafverfolgungsorgane bei einem kriminellen Hintergrund, durch die Offenlegung nicht gefährdet werden. Der Inhalt der Benachrichtigung variiert nach dem Empfänger. Die Benachrichtigung der Betroffenen muss für dessen Verständnishorizont eine Darlegung der Art der Verletzung und Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger

Folgen enthalten, z.B. beim Verlust von Bankdaten. Die Benachrichtigung der Aufsichtsbehörde muss eine Darlegung möglicher nachteiliger Folgen der Verletzung und der vom Betreiber nach der Verletzung ergriffenen Maßnahmen enthalten. Dies soll die Aufsichtsbehörde in den Stand versetzen, sicherzustellen, dass der datenschutzrechtliche Verstoß beseitigt wurde. Eine Benachrichtigung der Betroffenen kann für die verantwortliche Stelle einen unverhältnismäßigen Aufwand an Kosten und Zeit verursachen, z.B. bei einer vorherigen Ermittlung der Adressdaten der Betroffenen, sofern diese der verantwortlichen Stelle nicht bekannt sind. An Stelle der Benachrichtigung der Betroffenen, mit deren Inhalt, tritt eine Information der Öffentlichkeit. Dies wird durch Anzeigen, die mindestens eine halbe Druckseite umfassen, in mindestens zwei bundesweit erscheinenden Tageszeitungen sichergestellt. Eine entsprechende Unterrichtungspflicht von öffentlichen Stellen richtete sich u.a. auch analog zur Unterrichtungspflicht von auditierten Unternehmen nur an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, der den öffentlichen Bereich ständig überprüft.

Zu Nummer 10 (§ 47)

Die Vorschrift sieht eine Übergangsvorschrift … vor mit Blick auf die neuen Anforderungen an die Erhebung personenbezogener Daten. Mit dem Stichtag … gelten die neuen Anforderungen. Die betroffenen verantwortlichen Stellen werden daher bereits nach dem Inkrafttreten zum … beginnen müssen, ihre Datenerhebung schrittweise umzustellen.

Zu Artikel 2

Zu § 1 (Datenschutzaudit)

Die Durchführung des Datenschutzaudits ist freiwillig. Durch das Wort „können“ wird dies ausgedrückt. Es obliegt jedem Unternehmen zu entscheiden, ob den mit der Durchführung des Datenschutzaudits verbundenen Kosten und Mühen ein adäquater wirtschaftlicher Mehrwert aus der Verwendung des Datenschutzauditsiegels im Rechts- und Geschäftsverkehr gegenübersteht.

Adressat des Datenschutzaudits sind entsprechend § 9a Satz 1 des Bundesdatenschutzgesetzes Anbieter von Datenverarbeitungssystemen und -programmen und verantwortliche Stellen nach § 3 Abs. 7 des Bundesdatenschutzgesetzes. Anbieter stellen anderen, auch unentgeltlich, ein Datenverarbeitungssystem oder Datenverarbeitungsprogramm oder beides zur Verfügung, sei es als Hersteller oder in anderer Form am Vermarktungsprozess Beteiligter. Ein Datenverarbeitungssystem ist eine Funktionseinheit zur Verarbeitung von Daten. Der Begriff findet sich bereits verschiedentlich im Bundesdatenschutzgesetz, z.B. in §3a und Nummer 2, 3 und 5 Anlage zu § 9 Satz 1 und anderen Bundesgesetzen, z.B. in § 109 Abs. 1 Nr. 2, Abs. 2 Satz 1 des Telekommunikationsgesetzes, § 147 Abs. 6 Satz 1 der Abgabenordnung oder § 44 Abs. 2 Satz 1 des Außenwirtschaftsgesetzes. Datenverarbeitungsprogramme steuern die automatisierte Verarbeitung personenbezogener Daten. Auch dieser Begriff findet sich neben § 9a bereits verschiedentlich im Bundesdatenschutzgesetz, z.B. in § 4g Abs. 1 Satz 4 Nr. 1, § 24 Abs. 4 Satz 2 Nr. 1 und § 38 Abs. 4 Satz 2 sowie in anderen Bundesgesetzen, z.B. in § 4 Abs. 2 Nr. 3 des Außenwirtschaftsgesetzes (dort definiert als „Software“).

Einem Datenschutzaudit können sich Anbieter von Datenverarbeitungssystemen und -programmen und verantwortliche Stellen unterziehen, sofern sie „nicht-öffentliche Stelle im Sinne des § 2 Abs. 4 des Bundesdatenschutzgesetzes sind“. Die Einschränkung bezieht sich sowohl auf die Anbieter von Datenverarbeitungssystemen und -programmen als

auch die verantwortlichen Stellen. Ohne die Eingrenzung kämen auch öffentliche Stellen in Frage, die untereinander nicht im Wettbewerb stehen und bei denen die Bürgerinnen und Bürger nur in den seltensten Fällen ein Wahlrecht hätten, eine auditierte gegenüber einer nicht auditierten Stelle zu bevorzugen. Das Ziel, mit einem bundesweiten, gesetzlichen Datenschutzaudit wirtschaftliche Anreize zur Verbesserung des Datenschutzes und der Datensicherheit anzubieten, um hiermit nach außen im Wettbewerb zu werben und sich einen Marktvorteil zu verschaffen, würde insoweit verfehlt. Soweit eine öffentliche Stelle andere Zwecke verfolgt, etwa eine erhöhte Akzeptanz der Bürgerinnen und Bürger bei der Inanspruchnahme einer E-Government-Anwendung, wird dies bereits ausreichend dadurch gewährleistet, dass mit einem Datenschutzauditsiegel gekennzeichnete Datenschutzkonzepte und technische Einrichtungen eingesetzt werden können. Darüber hinaus bestehen Umsetzungsschwierigkeiten, da vorliegend nur Regelungen für öffentliche Stellen des Bundes getroffen werden könnten. Ausreichend ist daher, dass es weiterhin für öffentliche Stellen möglich bleibt, auf Landesebene ein Datenschutzaudit einzuführen, wie es z.B. in der Freien Hansestadt Bremen oder Schleswig-Holstein geschehen ist.

Gegenstand der Prüfung und Bewertung können Datenschutzkonzepte sowie technische Einrichtungen sein. In diesem Rahmen können die Unternehmen den Gegenstand des Audits selbst bestimmen und z.B. auf abgrenzbare Teilbereiche beschränken. Nicht nur die Durchführung des Audits überhaupt, sondern auch sein Umfang unterliegen auch wegen der damit verbundenen Kosten-Nutzen Abwägung der Dispositionsfreiheit der Unternehmen. Die Überprüfung eines gesamten Unternehmens im Rahmen eines Datenschutzaudits wird in aller Regel eine zu große Komplexität für eine Kontrolle aufweisen und ist allenfalls bei sehr kleinen Unternehmen vorstellbar, bei denen personenbezogene Daten nur zu einem Zweck oder wenigen klar umrissenen Zwecken durch ein einziges oder wenige einfach aufgebaute automatisierte Verfahren erhoben und verwendet werden.

Satz 2 verdeutlicht in Verbindung mit § 3 und § 11 die Voraussetzungen, unter denen ein Datenschutzauditsiegel verwendet werden darf.

Nach Nummer 1 sind die Vorschriften über den Datenschutz für die Datenverarbeitung einzuhalten, für die das Datenschutzkonzept oder die technische Einrichtung vorgesehen ist. Grundlage für die Verwendung ist also, dass die Datenverarbeitung, die Gegenstand des Datenschutzkonzepts oder der technischen Einrichtung ist gesetzeskonform betrieben wird. Andernfalls darf auch bei formaler Erfüllung der Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit nach Nummer 2 kein Datenschutzauditsiegel verwendet werden. Die Einhaltung der Vorschriften über den Datenschutz ist – vorbehaltlich der Nummer 3 – auf die Datenverarbeitung des Auditgegenstands beschränkt und nicht auf das Unternehmen als Adressaten des Audits insgesamt. Für die Kontrollstelle wäre es in aller Regel praktisch nicht umsetzbar, das Unternehmen als Ganzes auf die Einhaltung der Vorschriften über den Datenschutz zu überprüfen. Dies wäre unter Umständen auch nicht angemessen, wenn das Unternehmen lediglich für ein auf eine einzelne Datenverarbeitung bezogenes Datenschutzkonzept oder bezogene technische Einrichtung ein Datenschutzauditsiegel begehrt.

Nach Nummer 2 muss der Auditgegenstand die vom Datenschutzauditausschuss beschlossenen und veröffentlichen Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit nach § 11 Abs. 1 erfüllen. Ein Datenschutzauditsiegel, das lediglich das (gerade noch) Einhalten der Vorschriften über den Datenschutz (Gesetzeskonformität) verlangt, birgt verschiedene Probleme. Die Einhaltung der geltenden Gesetze wird von jedem Unternehmen erwartet und bedarf daher keiner Auszeichnung. Ein solches Datenschutzauditsiegel hätte für die Unternehmen auch keinen marktwirtschaftlichen Mehrwert gegenüber Wettbewerbern. Auf die Verbraucherinnen und Verbraucher hätte es im Gegenteil eine missverständliche Wirkung, da diese hinter einer staatlichen Auszeichnung eine überdurchschnittliche Leistung vermuten. Die Einhaltung der datenschutzrechtlichen Vorschriften bei den Unternehmen wird zudem bereits durch den Beauftragten für den Datenschutz nach § 4f Abs. 1 Satz 1 des Bundesdatenschutzgesetzes und die Aufsichts-

behörden nach § 38 des Bundesdatenschutzgesetzes kontrolliert. Ein auf die Gesetzeskonformität beschränktes Datenschutzauditsiegel läuft damit Gefahr, die bestehenden Kontrollen zu entwerten oder zumindest eine Verfahrensdoppelung herbeizuführen. Es besteht zudem die Gefahr, dass die Freiwilligkeit des Auditverfahrens in einen faktischen Zwang umschlägt, weil ein Unternehmen ohne ein Datenschutzauditsiegel für die Einhaltung der Gesetze den Rückschluss auf die Nichteinhaltung der Gesetze erlaubt. Ein Datenschutzkonzept oder eine technische Einrichtung muss nicht alle durch den Datenschutzauditausschuss erlassenen Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit erfüllen, sondern nur die für dieses Datenschutzkonzept oder diese technische Einrichtung geltenden. Sofern Richtlinien branchen- oder situationsspezifisch ausgerichtet sind, z.B. für den Bereich der Telekommunikationsunternehmen oder beschränkt auf Vorgaben der Protokollierung, finden sie keine Anwendung außerhalb dieses Bereichs oder sofern eine Protokollierung nicht erfolgt.

Nach Nummer 3 ist Voraussetzung für die Verwendung des Datenschutzauditsiegels, dass die Vorschriften des Bundesdatenschutzgesetzes über die organisatorische Stellung des Beauftragten für den Datenschutz eingehalten werden. Hierzu gehören insbesondere § 4f Abs. 3 und 5 des Bundesdatenschutzgesetzes. Nicht hierzu gehören die Vorschriften über seine fachliche Eignung; für das Berufsbild des Beauftragten für den Datenschutz bestehen derzeit noch keine tauglichen Kriterien. Zwar muss ein Unternehmen, um ein Datenschutzauditsiegel zu verwenden, nicht nachweisen und ständig kontrollieren lassen, dass es insgesamt die Vorschriften über den Datenschutz einhält. Diese Aufgabe obliegt innerbetrieblich nach § 4g Abs. 1 Satz 1 des Bundesdatenschutzgesetzes dem Beauftragten für den Datenschutz. Dieser kann seiner Aufgabe jedoch nur nachkommen und nach § 3 Satz 2 in die Durchführung des Kontrollverfahrens einbezogen werden, sofern seine organisatorische Stellung gesetzeskonform ausgestaltet ist und er z.B. die zur Erfüllung seiner Aufgaben erforderlichen Räume, Einrichtungen und Geräte zur Verfügung hat. Die Voraussetzungen für die Bestellung eines Beauftragten für den Datenschutz nach dem Bundesdatenschutzgesetz bleiben durch die Regelung unberührt.

Nach Nummer 4 ist Voraussetzung für die Verwendung des Datenschutzauditsiegels, dass die Nummern 1 bis 3 durch ein regelmäßiges Kontrollverfahren gemäß § 3 Satz 1 überprüft werden. Damit wird dem Umstand Rechnung getragen, dass Auditgegenstand sehr unterschiedliche und kurzlebige Verfahren und Produkte vor allem aus der dynamischen Informations- und Kommunikationsbranche sein werden. Die Vergabe eines Datenschutzauditsiegels aufgrund einer einmaligen Überprüfung läuft insoweit Gefahr, bereits kurze Zeit nach Abschluss des Verfahrens überholt zu sein. Normenklare Kriterien, wann und in welcher Intensität unter diesen Umständen ein erneutes Verfahren durchzuführen ist, lassen sich nur schwer bestimmen. Ein wiederholtes Verfahren mit Prüfungen nähert sich in tatsächlicher Hinsicht einem regelmäßigen Kontrollverfahren an. Dieses bietet mehr Flexibilität für die Durchführung der Kontrollen durch die Kontrollstellen und durch die Einbeziehung in das Kontrollsystem mehr Rechtssicherheit für das Unternehmen bei der Verwendung des Datenschutzauditsiegels. Für das Kontrollverfahren wird auf die Ausführungen zu § 3 Satz 1 verwiesen.

Soweit öffentliche Stellen als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen finden auf sie nach § 27 Abs. 1 Satz 1 Nr. 2 des Bundesdatenschutzgesetzes dieselben Vorschriften Anwendung, wie auf nicht-öffentliche Stellen. Sie sind diesen gleichgestellt. Im Wettbewerb mit nicht-öffentlichen Stellen soll ihnen kein Nachteil durch die strengeren Regelungen für öffentliche Stellen entstehen. Aus dieser wettbewerbsbedingten Gleichstellung folgt, dass auch öffentlich-rechtlichen Wettbewerbsunternehmen die Möglichkeit eröffnet werden muss, sich durch ein Datenschutzauditsiegel einen werbewirksamen Marktvorteil gegenüber seinen nicht-öffentlichen Konkurrenten zu verschaffen.

Zu § 2 (Zuständigkeit)

Absatz 1:

Die Zuständigkeit für die Erfüllung staatlicher Aufgaben liegt nach Artikel 30 Grundgesetz grundsätzlich bei den Ländern. Dies wird durch Satz 1 klargestellt. Zugleich soll das Verfahren der Kontrolle mit § 3 in weitem Umfang zugelassenen privaten Kontrollstellen übertragen werden. Zu weiteren Einzelheiten wird auf die Ausführungen zu § 3 verwiesen. Satz 2 dient der Anpassung der Zuständigkeitsverteilung an die spezialgesetzliche Regelung in § 115 Abs. 4 des Telekommunikationsgesetzes und § 42 Abs. 3 des Postgesetzes. Danach ist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zuständige Aufsichtsbehörde für den Datenschutz, soweit für die geschäftsmäßige Erbringung von Post- oder Telekommunikationsdiensten Daten zu natürlichen oder juristischen Personen erhoben, verarbeitet oder genutzt werden.

Absatz 2:

Mit Absatz 2 werden bestimmte Aufgaben beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit gebündelt. Eine Vielzahl von Unternehmen, für die das Datenschutzaudit interessant ist, haben Niederlassungen in verschiedenen Ländern und sind interessiert, sich nur von einer Kontrollstelle kontrollieren zu lassen. Auch die Kontrollstellen haben ein Interesse an einer länderübergreifenden Tätigkeit. Dafür ist eine grundsätzlich bundesweit geltende Zulassung erforderlich, die mit dem Ziel eines effizienten Verfahrens nur von einer zentralen, mit alleiniger Entscheidungskompetenz ausgestatteten Stelle erteilt werden kann. Das Zulassungsverfahren und die Entscheidung über die Entziehung der Zulassung einer Kontrollstelle sollen durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wahrgenommen werden. Folgerichtig ist auch die Zuständigkeit für die Erteilung der Kennnummer an die zugelassenen Kontrollstellen mit Nummer 2 dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zuzuweisen. Zu Einzelheiten des Verfahrens der Zulassung und der Entziehung der Zulassung wird auf die Ausführungen zu § 4 Abs. 1 und § 4 Abs. 4 verwiesen.

Zu § 3 (Kontrollen)

Nachdem in § 2 Abs. 1 Satz 1 und 2 die Zuständigkeit der Länder und des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit für die Durchführung des Gesetzes klargestellt ist, soll Satz 1 dem Bestreben nach einer möglichst weitgehenden Aufgabenerledigung durch Private Rechnung tragen, ohne besonders einschneidende hoheitliche Entscheidungen aus dem behördlichen Aufgabenbereich auszugliedern. Vom behördlichen Aufgabenbereich erfasst sind insbesondere die Maßnahmen, mit denen die zuständigen Behörden sicherstellen, dass bei Unregelmäßigkeiten oder Verstößen keine Kennzeichnung mit dem Datenschutzauditsiegel erfolgt. Mit dieser Ausgestaltung soll das in Deutschland und der überwiegenden Zahl der Mitgliedstaaten der Europäischen Union seit längerem praktizierte und funktionierende System auf dem Gebiet des ökologischen Landbaus für den Bereich des Datenschutzes nutzbar gemacht werden.

Nach Satz 2 ist der Beauftragte für den Datenschutz gemäß § 4f Abs. 1 Satz 1 des Bundesdatenschutzgesetzes in die Durchführung der Kontrollen einzubeziehen. Damit soll seiner zentralen Rolle innerhalb des Unternehmens bei der Einhaltung des Bundesdatenschutzgesetzes und anderer Vorschriften über den Datenschutz, insbesondere im Rahmen der Vorabkontrolle Rechnung getragen werden. Die Einbeziehung des Beauftragten für den Datenschutz in die Durchführung von Kontrollen durch unternehmensexterne Stellen sollte vor dem Hintergrund seiner gesetzlichen Aufgaben und sachlichen Kompetenz selbstverständlich sein. Die Regelung hat daher vorwiegend klarstellenden Charakter. Der Beauftragte für den Datenschutz wird bereits jetzt bei Kontrollen der Aufsichtsbehörden einbezogen. Wie dort, umfasst die Einbeziehung etwa die Vorbereitung und Koordination der zur Durchführung der Kontrollen notwendigen Arbeitsschritte, von der Bestandsaufnahme über die Aufbereitung der erforderlichen Unterlagen und Vermittlung von Ansprechpartnern im Betrieb bis hin zur Beseitigung von festgestellten Mängeln. Die Einbeziehung in die Durchführung der Kontrollen verdeutlicht, dass der Beauftragte für den Datenschutz nicht selbst, etwa seine Eignung, Gegenstand der Kontrolle ist. Satz 2 lässt im

Übrigen die Regelungen zur Bestellung eines Beauftragten für den Datenschutz nach dem Bundesdatenschutzgesetz unberührt und führt nicht zu einer abweichenden Verpflichtung zur Bestellung bei Durchführung eines Datenschutzaudits.

Das Verfahren der Kontrolle muss die in der Verordnung nach § 16 Abs. 3 Nr. 3 näher auszuführenden Kontrollanforderungen und Mindeststandards erfüllen. Dabei ist der dort vorzusehende Kontrollrahmen mit Rücksicht auf die konkreten Bedingungen im Zusammenspiel von Kontrollstelle und kontrollierter Stelle zu spezifizieren. Die Art und Häufigkeit der Kontrollen soll sich nach Satz 3 nach dem Risiko des Auftretens von Unregelmäßigkeiten und Verstößen in Bezug auf die Erfüllung der Anforderungen dieses Gesetzes und der auf Grund dieses Gesetzes erlassenen Rechtsverordnungen bestimmen, wobei jedoch jedes in das Kontrollsystem einbezogene Unternehmen mindest einmal jährlich überprüft werden soll. Die auf Grundlage des Bundesdatenschutzgesetzes und der Datenschutzgesetze der Länder durchgeführten Kontrollen bleiben von der Übertragung des Verfahrens der Kontrolle auf zugelassene private Kontrollstellen unberührt.

Zu § 4 (Zulassung der Kontrollstellen und Entziehung der Zulassung)

Absatz 1:

Werden wesentliche Teile des Kontrollverfahrens auf Private übertragen, muss die Zulassung der Privaten vorgeschrieben sein, um die ordnungsgemäße Aufgabenerledigung durch diese sicherzustellen und zu gewährleisten, dass die an sie gestellten Anforderungen erfüllt werden. Die Kontrollstellen bilden den Kern des Kontrollsystems. Von der Qualität ihrer Tätigkeit hängen die Zuverlässigkeit sowie die Funktion des gesamten Kontrollverfahrens und damit das Niveau der Auditierung maßgeblich ab. Diesen Erfordernissen trägt § 4 Abs. 1 Rechnung. Kontrollstellen sind zuzulassen, wenn sie für ihr Leitungspersonal und ihre für Kontrollen verantwortlichen Beschäftigten eine persönliche Zuverlässigkeit, Unabhängigkeit und fachliche Eignung nachweisen, die näher in § 9 aufgeführt ist. In organisatorischer Hinsicht muss die Kontrollstelle den Anforderungen der bei der Beuth Verlag GmbH, Berlin, zu beziehenden und beim Deutschen Patentamt archivmäßig gesichert niedergelegten DIN EN 45011 (Allgemeine Anforderungen an Stellen, die Produktzertifizierungssysteme betreiben) genügen und dies durch eine entsprechende Akkreditierung nachweisen, wie in verschiedenen anderen Bereichen bereits praktiziert. Ergänzend wird neben der Entrichtung der Zulassungsgebühren das Unterhalten ihres Sitzes oder einer Niederlassung im Inland zur Bedingung für die Zulassung gemacht. Nur unter dieser Bedingung lässt sich die Aufsicht über die Kontrollstellen, die den zuständigen Behörden im Einzelnen auferlegt ist, zuverlässig und wirksam sicherstellen.

Absatz 2:

Absatz 2 Satz 1 regelt die mit der zentralen Zulassung durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit eröffnete Möglichkeit, eine bundesweite Zulassung zu erteilen. Satz 2 reduziert Verwaltungsaufwand bei solchen Kontrollstellen, die nur in einem beschränkten Gebiet tätig sein wollen. Die Kontrollstellen unterliegen dann in Ländern, in denen sie nicht zugelassen sind, auch nicht dem Kontrahierungszwang nach § 5 Abs. 1.

Absatz 3:

Verfahren im Hinblick auf den Entzug der Zulassung einer unzuverlässig arbeitenden Kontrollstelle können einen erheblichen Zeitraum in Anspruch nehmen. In dieser Zeit ist die Kontrollstelle in der Regel weiterhin tätig und stellt ein Risikoelement für die Integrität des Kontrollsystems und die Aussagekraft des Datenschutzauditsiegels dar. Damit die zuständigen Behörden im Bedarfsfall schnell und effektiv eingreifen können, bieten Befristungen, Bedingungen, Auflagen und Widerrufsvorbehalte die Möglichkeit, entsprechende Vorkehrungen zu treffen, um dem entgegenzuwirken und die Belange des Datenschutzes

sicherzustellen. Durch die Worte „soweit es die Aufrechterhaltung der Funktionsfähigkeit des Kontrollsystems“ erfordert, soll der landesrechtlichen Möglichkeit zur Beleihung oder Mitwirkung durch eine Nebenbestimmung bei der Zulassung der Kontrollstelle Rechnung getragen werden. Eine Zulassung, mit der die Befähigung einer Kontrollstelle zur Wahrnehmung der Kontrollaufgaben festgestellt wird, kann ihre Wirkungen nur unter der Bedingung entfalten, dass die Aufgabenübertragung in dem betreffenden Land erfolgt. Die Bereitschaft einer Kontrollstelle, sich den Landesbestimmungen zur Beleihung oder Mitwirkung zu unterwerfen, ist Kriterium dafür, ob die Kontrollstelle zu einer ordnungsgemäßen und koordinierten Durchführung des Kontrollverfahrens in der Lage ist. Dem folgt der Absatz 3, indem er der für die Zulassung der Kontrollstellen zuständigen Behörde, dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, die Möglichkeit eröffnet, die Zulassung mit Nebenbestimmungen zu versehen.

Absatz 4:

Ein Entzug der Zulassung ist in zwei Konstellationen zulässig: Wenn die Kontrollstelle die Voraussetzungen für die Zulassung nicht mehr erfüllt und wenn sie Verpflichtungen nach diesem Gesetz oder einer aufgrund dieses Gesetzes erlassenen Rechtsverordnung in schwerwiegender Weise nicht nachkommt. Die Hervorhebung der Verpflichtungen gegenüber der sie überwachenden zuständigen Behörde erfolgt, da diese für das Kontrollsystem insgesamt von besonderer Bedeutung sind. Die Eingrenzung auf Verpflichtungen, denen in schwerwiegender Weise nicht nachgekommen wird, soll verdeutlichen, dass nicht jede Unregelmäßigkeit der Kontrollstelle die besonders schwere Sanktion des Entzugs der Zulassung nach sich ziehen soll, z.B. dann, wenn die Unregelmäßigkeit nicht verschuldet ist, erstmalig auftritt oder substanzielle Änderungen nach sich gezogen hat.

Zu § 5 (Pflichten der Kontrollstelle)

Absatz 1:

Mit Absatz 1 wird Rechnung getragen, dass sicherzustellen ist, dass ein Unternehmen, das die Bestimmungen des Gesetzes einhält und seinen Beitrag zu den Kosten des Kontrollverfahrens entrichtet, einen Anspruch hat, in das Kontrollsystem einbezogen zu werden. Die Einschränkung der Bedingungen, unter denen ein Unternehmen in die Kontrollen einer Kontrollstelle einzubeziehen ist, in Bezug auf die tatsächliche Zulassung dieser Kontrollstelle in dem betroffenen Land, soll der Regelung nach § 4 Abs. 3 Satz 1 (soweit es die Aufrechterhaltung der Funktionsfähigkeit des Kontrollsystems erfordert) Rechnung tragen. Nach dieser Bestimmung kann die Zulassung auf Antrag auf einzelne Länder beschränkt oder für Länder, in denen eine Beleihung vorgesehen ist, unter der aufschiebenden Bedingung erteilt werden, dass die Beleihung erfolgt. Es besteht insoweit im zweiten Fall die Möglichkeit, dass eine Kontrollstelle in bestimmten Ländern, solange die aufschiebende Bedingung nicht eintritt, nicht zur Durchführung von Kontrollen zugelassen ist. Diese Tatsache ist als Ablehnungsgrund zu berücksichtigen. Weitere von der Kontrollstelle vorgebrachte Gründe für eine Ablehnung des Verlangens eines Unternehmens, in die Kontrollen einbezogen zu werden, sollen nach Satz 2 Nr. 1 unter den Entscheidungsvorbehalt der nach Landesrecht zuständigen Behörde gestellt werden. Der Kontrahierungszwang für die Kontrollstellen kann nur dann gelockert werden, wenn die Kontrolle durch andere Kontrollstellen sichergestellt ist. Diesem Erfordernis soll in Nummer 2 Rechnung getragen werden, indem diese Sicherstellung der Durchführung des Kontrollverfahrens für das Unternehmen als Voraussetzung für die Ausnahme vom Kontrahierungszwang formuliert wird.

Absatz 2:

Die Kontrollstelle übermittelt den zuständigen Behörden jährlich spätestens bis zum 31. Januar ein Verzeichnis der Unternehmen, die am 31. Dezember des Vorjahres ihrer Kontrolle unterstanden. Die Kontrollstelle legt ferner bis spätestens zum 31. März jedes Jah-

res einen zusammenfassenden Bericht über die im Vorjahr ausgeführte Kontrolltätigkeit vor, wobei insbesondere alle festgestellten Abweichungen, Unregelmäßigkeiten und Verstöße sowie die getroffenen Maßnahmen zu dokumentieren sind.

Absatz 3:

Die in Absatz 3 vorgesehene Mitteilungspflicht wird den Kontrollstellen auferlegt, damit das Sanktionssystem mit arbeitsteiliger Aufgabenwahrnehmung zwischen privater Kontrollstelle und zuständiger Behörde funktioniert. Satz 1 soll die direkte und effektive Zusammenarbeit der Kontrollstellen zur ordnungsgemäßen Durchführung des Kontrollsystems sicherstellen. Die Bestimmung entbindet die Kontrollstellen nicht von ihrer Meldepflicht gegenüber den zuständigen Behörden nach Satz 2. Mit Satz 3 sollen die Melde- und Informationspflichten der Kontrollstellen für den Fall präzisiert werden, dass sich ein begründeter Verdacht auf Unregelmäßigkeiten oder Verstöße gegenüber einem nicht von dieser Kontrollstelle kontrollierten Unternehmen ergibt. Satz 3 macht zudem deutlich, dass sich die Kontrollstelle bei gegebener Veranlassung auch mit der Frage zu befassen hat, ob die bei dem kontrollierten Unternehmen festgestellte Unregelmäßigkeit ihren Ursprung bei einem anderen Unternehmen hat. Diese Frage ist immer dann nachzugehen, wenn die Feststellungen der Kontrollstelle eine Zuwiderhandlung bei einem vorgelagerten Arbeitsschritt erkennen lassen, so dass eine Rückverfolgung notwendig ist. Unterliegt das für den vorgelagerten Arbeitsschritt verantwortliche Unternehmen ebenfalls der Überwachung durch die Kontrollstelle, gilt der Satz unmittelbar. Ist das nicht der Fall muss die Kontrollstelle die nach Landesrecht zuständige Behörde für das für den vorgelagerten Arbeitsschritt verantwortliche Unternehmen über ihre Feststellungen unterrichten. Soll ein Datenschutzauditsiegel z.B. für ein Datenverarbeitungssystem verwendet werden, das teilweise auf Geräten oder Datenverarbeitungsprogrammen mit Datenschutzauditsiegel basiert oder diese mit einbezieht und ergibt sich für die Kontrollstelle in Bezug auf diese Geräte oder Datenverarbeitungsprogramme ein begründeter Verdacht auf Unregelmäßigkeiten oder Verstöße, die jedoch Unternehmen außerhalb seiner Zuständigkeit betreffen, so hat die Kontrollstelle die zuständige Kontrollstelle zu unterrichten. Diese Pflicht muss schon bei dem begründeten d.h. auf Tatsachen gestützten Verdacht einer Unregelmäßigkeit oder eines Verstoßes eingreifen, weil die unterrichtende Kontrollstelle mangels eigener Zuständigkeit keine abschließende Prüfung bei dem für den vorgelagerten Arbeitsschritt verantwortlichen Unternehmen durchführen kann.

Absatz 4:

Absatz 4 enthält Vorschriften zum Schutz der kontrollunterworfenen Unternehmen, denen im Fall der Einstellung der Tätigkeit der sie bisher kontrollierenden Stelle, auch im Falle einer Insolvenz, Gelegenheit gegeben werden soll, die weitere Teilnahme am Kontrollverfahren – möglichst ohne zeitliche Unterbrechung – sicherzustellen.

Zu § 6 (Pflichten der zuständigen Behörde)

Absatz 1:

Mit Absatz 1 soll das arbeitsteilige Verfahren der Überwachung der in den einzelnen Ländern tätigen Kontrollstellen durch die zuständigen Behörden geregelt werden. Die zuständige Behörde veranlasst nach Satz 1 bei Bedarf Überprüfungen und Inspektionen der Kontrollstelle. Derartige Überprüfungen können auch ohne Anlass erfolgen. Satz 2 regelt die gegenseitigen Unterrichtungs- und Auskunftspflichten der zuständigen Behörden im Rahmen der Überwachung der Kontrollstellen. Die Vorschrift stellt die notwendige Ergänzung für eine sachgerechte und wirksame Überwachung im Hinblick auf die Regelung in § 2 Abs. 2 Nr. 1 dar, nach der die Kontrollstellen nach Zulassung durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit grundsätzlich bundesweit tätig werden können. Der Entzug der Zulassung einer Kontrollstelle nach § 4 Abs. 4 resultiert regelmäßig aus dem Überwachungsverfahren, das nach Satz 1 den zuständigen Behör-

den der Länder obliegen soll. Damit der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit über den Entzug der Zulassung entscheiden kann, muss die für die Überwachung zuständige Landesbehörde nach der Feststellung von Verstößen einer Kontrollstelle, die den Entzug der Zulassung rechtfertigen, den Entzug der Zulassung beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit anregen. Dem wird durch Satz 3 und 4 Rechnung getragen. Stellt die zuständigen Behörde für eine Kontrollstelle, die augrund ihres Sitzes ihrer Aufsicht unterliegt, Tatsachen fest, die den Entzug der Zulassung oder die Aufnahme oder Änderung von Auflagen zur Zulassung erforderlich machen können, hat sie unmittelbar den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit diese Tatsachen mitzuteilen und anzuregen, ein Verfahren zum Entzug der Zulassung oder zur Aufnahme oder Änderung von Auflagen einzuleiten. Beziehen sich die Tatsachen auf eine Kontrollstelle, die aufgrund ihres Sitzes der Aufsicht einer anderen zuständigen Behörde unterliegt, hat sie dieser die Tatsachen mitzuteilen. Nach Satz 4 trifft dann diese andere zuständige Behörde die Verpflichtung zur Mitteilung an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und zur Anregung, ein Verfahren zum Entzug der Zulassung oder zur Aufnahme oder Änderung von Auflagen einzuleiten. Der für den Sitz der jeweiligen Kontrollstelle zuständigen Landesbehörde wird damit eine Schlüsselrolle sowohl bei der Koordinierung der Überwachung als auch bei der Entscheidung über die Änderung von Nebenbestimmungen zur Zulassung oder den Entzug der Zulassung durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zugewiesen. Satz 5 ist der abweichenden Zuständigkeit nach § 2 Abs. 1 Satz 2 in Bezug auf den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit geschuldet, der insoweit die Überwachung der Kontrollstellen nach Satz 1 übernimmt.

Absatz 2:

Da die aufgeführten hoheitlichen Maßnahmen erheblich in die Rechte der betroffenen Unternehmen eingreifen, sollen sie grundsätzlich den nach Landesrecht zuständigen Behörden bzw. im Rahmen des § 2 Abs. 1 Satz 2 dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vorbehalten bleiben. Dabei ist den zuständigen Behörden Ermessen eingeräumt, ob und in welcher Weise sie vorgehen. Dabei sollen unter anderem die Bedeutung der Vorschrift, gegen die verstoßen wurde, sowie die Art und die besonderen Umstände der Unregelmäßigkeit einbezogen werden. Bei schwerwiegenden Verstößen oder Verstößen mit Langzeitwirkung, kann die Kennzeichnung für eine mit der zuständigen Behörde zu vereinbarende Dauer untersagt werden, z.B. weil es zunächst erforderlich ist, ein Produkt oder Verfahren technisch nachzubessern oder organisatorische Maßnahmen umzusetzen.

Zu § 7 (Überwachung)

Zur Durchführung der Überwachung des Datenschutzauditgesetzes und der auf Grund dieses Gesetzes erlassenen Rechtsverordnungen ist es erforderlich, dass den hierzu Beauftragten auf Verlangen die entsprechenden Auskünfte erteilt werden. Ferner sind sie mit entsprechenden Rechten, insbesondere dem Betretungs- und Besichtigungsrecht sowie dem Einsichts- und Prüfungsrecht auszustatten, denen entsprechende Rechte und Pflichten der Betroffenen gegenüber stehen. Damit lehnt sich die Regelung an bewährte Vorschriften zur Überwachung in anderen Regelungsbereichen an, insbesondere den Befugnissen der Aufsichtsbehörden nach § 38 Abs. 3 und 4 des Bundesdatenschutzgesetzes. Die Regelung umfasst die Überwachung der Kontrollstellen und in diesem Zusammenhang der kontrollierten Unternehmen durch die zuständigen Behörden. Ferner bedarf es einer entsprechenden Regelung für das Verhältnis der zugelassenen Kontrollstellen gegenüber den in das Kontrollverfahren einbezogenen Unternehmen. Die in Absatz 2 aufgeführten Befugnisse der Personen, die von der zuständigen Behörde beauftragt sind, begründen lediglich die Duldungspflichten nach Absatz 3, beschreiben jedoch insoweit nicht abschließend den Inhalt der Tätigkeiten, zu denen die genannten Personen befugt sind.

Zu § 8 (Datenschutzauditsiegel, Verzeichnisse)

Absatz 1:

Mit einem Datenschutzauditsiegel nach Maßgabe einer Rechtsverordnung nach § 16 Abs. 4 Nr. 1 dürfen Datenschutzkonzepte sowie technische Einrichtungen nur gekennzeichnet werden, wenn die Voraussetzungen für die Verwendung des Datenschutzauditsiegels nach § 1 Satz 2 erfüllt sind.

Absatz 2:

Absatz 2 verfolgt das Ziel, das Internet und den elektronischen Bundesanzeiger zur Feststellung der Echtheit von mit einem Datenschutzauditsiegel gekennzeichneten Datenschutzkonzepten oder technischen Einrichtungen zu nutzen. Damit werden Erfahrungen, u. a. in Bezug auf die Ursachen von Betrugsfällen im Bereich der Vergabe von Bio-Siegeln aufgegriffen. Satz 1 verpflichtet jedes Unternehmen, das ein Datenschutzkonzept oder eine technische Einrichtung verwenden möchte, dies bei dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit anzuzeigen. Näheres zu der Anzeige und den verpflichtenden Angaben regelt eine Rechtsverordnung nach § 16 Abs. 3 Nr. 5. Für die lückenlose Kontrolle und Überwachung ist es notwendig, dass die Anzeige noch vor der ersten Verwendung erfolgt. Nach den Sätzen 2 bis 4 hat der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ein Verzeichnis der angezeigten Datenschutzkonzepte oder technischen Einrichtungen des anzeigenden Unternehmens sowie der Kontrollstelle zu führen und auf seiner Internetseite und im elektronischen Bundesanzeiger zum Zwecke der Information der zuständigen Behörden und Betroffenen verfügbar zu machen. Mit dem Verzeichnis wird für diese aber auch andere Wirtschaftsbeteiligte eine Informationsmöglichkeit geschaffen, um sichere Auskünfte über die Echtheit der betroffenen Datenschutzkonzepte sowie technischen Einrichtungen zu erhalten. Soweit das Verzeichnis Informationen über die von den Kontrollstellen kontrollierten Unternehmen enthält, beugt es Verfälschungen und Missbrauch von Datenschutzauditsiegeln vor und verbessert bei geringem Aufwand den Schutz der Betroffnen. Die Informationen sind auch für Vertragspartner unverzichtbar, um zuverlässig prüfen zu können, ob das betreffende Unternehmen aktuell berechtigt ist, für ein bestimmtes Datenschutzkonzept oder eine technische Einrichtung ein Datenschutzauditsiegel zu verwenden.

Absatz 3:

Absatz 3 sieht in gleicher Weise wie in Absatz 2 ein Verzeichnis vor, in dem der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit die von ihm zugelassenen Kontrollstellen mit Namen und Anschrift sowie der ihnen erteilten Kennnummer aufführt. Kontrollstellen, denen die Zulassung entzogen worden sind, werden nicht mehr aufgeführt. Damit wird es u. a. den Unternehmen ermöglicht, für sie in Frage kommende Kontrollstellen ausfindig zu machen.

Zu § 9 (Anforderungen an Kontrollstellen)

Die Vorschrift regelt im Einzelnen die Anforderungen an Kontrollstellen zum Nachweis der nach § 4 Abs. 1 Nr. 1 geforderten Zuverlässigkeit, Unabhängigkeit und fachlichen Eignung. Sie orientiert sich an den Regelungen der §§ 5 bis 7 des Umweltauditgesetzes zu der von Umweltgutachtern geforderten Zuverlässigkeit, Unabhängigkeit und Fachkunde und der von Beauftragten für den Datenschutz nach § 4f Abs. 1 Satz 1 geforderten Zuverlässigkeit und erforderlichen Fachkunde sowie vergleichbaren Landesregelungen. Die Anforderungen werden an das Leitungspersonal der Kontrollstelle und die für Kontrollen verantwortlichen Beschäftigen gestellt. Eine Beschränkung allein auf das Leitungspersonal birgt die Gefahr, dass die konkret für die Kontrolle verantwortlichen Beschäftigten z.B. mangels fachlicher Eignung, die Erfüllung der Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit nicht überprüfen oder bestätigen können. Eine Erstre-

ckung der Anforderungen auf weitere Beschäftigte, die keine Verantwortung für die Kontrollen tragen, ist nicht erforderlich und angemessen.

Zu § 10 (Gebühren und Auslagen)

Die Vorschrift normiert ausschließlich die Erhebung von Gebühren und Auslagen für Amtshandlungen von Bundesbehörden; Gebühren- und Auslagenregelungen für Leistungen der Länderbehörden werden dagegen einer landesrechtlichen Regelung überlassen.

Absatz 1:

Absatz 1 schafft eine auf den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit beschränkte Gebühren- und Auslagenregelung.

Satz 1 legt den Umfang der gebühren- und auslagenpflichtigen Amtshandlungen fest. Die Gebührenpflicht erfasst Amtshandlungen des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit nach § 2 Abs. 1 Satz 2 und Abs. 2. Damit sind auch die Zulassung einer Kontrollstelle, die Entziehung dieser Zulassung und die Vergabe einer Kennnummer an die Kontrollstelle in die Gebührenpflicht einbezogen. Ferner erfasst die Gebührenpflicht Amtshandlungen nach § 8 Abs. 2 und 3. Dazu zählen die Entgegennahme der Anzeige der Verwendung des Datenschutzauditsiegels sowie die Aufnahme der angezeigten Datenschutzkonzepte und technischen Einrichtungen und weiterer Daten in einem Verzeichnis im Internet umfassen soll, Gebühren und Auslagen zu erheben.

Für die Bemessung der Gebühren ordnet Satz 1 das Kostendeckungsprinzip an. Damit gilt nach § 3 Abs. 2 des Verwaltungskostengesetzes das Verbot der Kostenüberdeckung, wonach Gebühren so bemessen sein müssen, dass das geschätzte Gebührenaufkommen den auf die Amtshandlung entfallenden durchschnittlichen Personal- und Sachaufwand für den betreffenden Verwaltungszweig nicht übersteigt. Die Erhebung von Verwaltungsgebühren zur Erzielung von Überschüssen ist damit nicht gestattet. Bei der Kalkulation der Kosten kann der gesamte auf die einzelne gebührenpflichtige Leistung entfallende Verwaltungsaufwand berücksichtigt werden.

Die näheren Bestimmungen zur Gebühren- und Auslagenerhebung werden nach den Sätzen 2 und 3 durch Rechtsverordnung des Bundesministeriums des Innern getroffen.

Absatz 2:

Die Vorschrift stellt klar, dass die Regelung der Gebühren und Auslagen für Amtshandlungen der Landesbehörden nach § 6 Abs. 1 Satz 1 und Abs. 2 den Ländern obliegt.

Zu § 11 (Datenschutzauditausschuss)

Absatz 1:

Nach Absatz 1 Satz 1 wird beim Bundesbeauftragten für den Datenschutz ein Datenschutzauditausschuss eingerichtet.

Satz 2 bestimmt die Aufgabe des Datenschutzauditausschusses, Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit zu erlassen. Einige Mittel durch die Richtlinien über den bestehenden Stand der Gesetze hinaus Verbesserungen des Datenschutzes und der Datensicherheit erreichen können, sind nicht abschließend aufgeführt. Die Aufzählung berührt nicht die Entscheidung des Ausschusses, welche Richtlinien er inhaltlich vorrangig angeht und mit welchen Mitteln er eine Verbesserung des Datenschutzes und der Datensicherheit anstrebt.

Die Beachtung der in den Richtlinien enthaltenen Kriterien wird von den zugelassenen Kontrollstellen im Rahmen ihrer Kontrollen nach Maßgabe dieses Gesetzes überprüft. Zudem kann es, etwa bei der Aktualisierung von überholten Richtlinien, notwendig sein, nachzuweisen, ab welchem Zeitpunkt die Richtlinie veröffentlicht war und von der zugelassenen Kontrollstelle und dem kontrollierten Unternehmen zu beachten war. Die Richtlinien sind daher nach Satz 3 über die Veröffentlichung auf der Webseite des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und im elektronischen Bundesanzeiger bekannt zu machen.

Absatz 2:

Nach Absatz 2 erstellt der Datenschutzauditausschuss jährlich einen Bericht über seine Tätigkeit, z.B. Umfang, Inhalt und Probleme und Erfahrungen, insbesondere über die Praktikabilität und erforderliche Änderungen erlassener Richtlinien und den Bedarf für neue Richtlinien. Der Bericht stärkt die Transparenz der Arbeiten des Ausschusses. Der Ausschuss hat nach seiner gesetzlichen Aufgabe, Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit, die Möglichkeit, Diskussionen zu datenschutzrechtlichen Themen anzustoßen, die zur Fortentwicklung des Datenschutzes beitragen. Im Bericht können ferner Richtlinien in einer Weise erläutert werden, wie es im Rahmen der amtlichen Bekanntmachung nicht möglich ist. Durch die Ankündigung, neue Richtlinien für weitere Bereiche zu erlassen oder erlassene Richtlinien anzupassen, können die betroffenen Unternehmen und zugelassenen Kontrollstellen sich bereits frühzeitig einstellen.

Zu § 12 (Mitglieder des Datenschutzauditausschusses)

Absatz 1:

Absatz 1 Satz 1 regelt die Zusammensetzung des Datenschutzauditausschusses und die Verteilung der 18 Mitglieder auf die im Ausschuss vertretenen Gruppen.

Der Datenschutzauditausschuss soll nach Größe und Zusammensetzung ausgewogen mit praxisorientierten, wirtschaftsnahen Mitgliedern und Mitgliedern der Verwaltung mit Bezug zum Datenschutz und der Datensicherheit sowie dem Datenschutzauditverfahren besetzt sein. Demnach sind im Datenschutzauditausschuss vertreten:

- Vertreter der Verwaltung des Bundes und der Länder, da sie in verschiedener Weise für fachspezifische Vorschriften des Datenschutzes zuständig sind,

- Vertreter des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, da er die Kontrollstellen zulässt und die Zulassung entzieht und um aus seinem Zuständigkeitsbereich aufsichtsbehördliche Erkenntnisse zur Lage des Datenschutzes und zu dessen Verbesserung einzubringen,

- Vertreter des Bundesamtes für Sicherheit in der Informationstechnik, da es aufgrund seiner gesetzlichen Aufgaben eine hervorgehobene Rolle im Bereich der Datensicherheit spielt und um Aspekte der Datensicherheit einzubringen,

- Vertreter von Aufsichtsbehörden der Länder für den Datenschutz im nicht-öffentlichen Bereich, da sie die ordnungsgemäßen Kontrollen der Kontrollstellen überwachen und, um aufsichtsbehördliches Erkenntnisse zur Lage des Datenschutzes und zu dessen Verbesserung einzubringen,

- Vertreter von Unternehmen, da sie sich zur Verwendung des Datenschutzauditsiegels in das Kontrollverfahren einbeziehen lassen und branchenspezifische sowie aus der Anwendung gewonnene Aspekte beitragen können.

Kriterien für die zahlenmäßige Zusammensetzung des Datenschutzauditausschusses sind die Arbeitsfähigkeit des Ausschusses, eine Abstufung der Mitgliederzahl entsprechend der unterschiedlichen Betroffenheit der vertretenen Gruppen und unter Berücksichtigung der Sperrminorität nach § 13 Abs. 3 Nr. 1.

Die größte Einzelgruppe stellen die sechs Vertreter von Unternehmen. Eine zu stark aufsichtsbehördliche Zusammensetzung läuft Gefahr, Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit zu erlassen, die eine sehr hohe Qualität gewährleisten und das Vertrauen der Verbraucherinnen und Verbraucher genießen, jedoch praktischen Bedürfnissen der Unternehmen nicht genügend Rechnung tragen und daher keine Verbreitung finden. Damit ginge auch der Mehrwert für die Fortentwicklung des Datenschutzes, insbesondere in der Breite, verloren. Ziel des Ausschusses kann es allerdings nicht sein, Richtlinien zu erlassen, die keine substanzielle Verbesserung des Datenschutzes erreichen. Derartige Richtlinien würden letztlich das Datenschutzauditsiegel entwerten, bei Verbraucherinnen und Verbrauchern auf Ablehnung stoßen und damit auch den angestrebten Mehrwert für die Wirtschaft mindern. Aus diesem Grund sind die Datenschutzaufsichtsbehörden mit insgesamt sechs Vertretern in gleicher Stärke vertreten wie die Unternehmensvertreter. Vertreter des Bundesamtes für Sicherheit in der Informationstechnik sind in derselben Größenordnung wie der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit vertreten, um die Datensicherheit als Bestandteil des Datenschutzes (§ 9 des Bundesdatenschutzgesetzes) hervorzuheben und Reibungsverluste mit der Tätigkeit des Bundesamtes für Sicherheit in der Informationstechnik zu vermeiden.

Satz 2 bestimmt, dass die Mitglieder des Datenschutzauditausschusses keinen Weisungen unterliegen und ehrenamtlich tätig sind.

Durch Satz 3, der die §§ 83, 84 Verwaltungsverfahrensgesetz für anwendbar erklärt, werden die ehrenamtlich tätigen Mitglieder auf Gewissenhaftigkeit, Unparteiischkeit und Verschwiegenheit verpflichtet. Da § 85 Verwaltungsverfahrensgesetz nicht für anwendbar erklärt wird, sind Auslagen und Verdienstausfall der Ausschussmitglieder nicht vom Bund, sondern in der Regel von der entsendenden Institution zu ersetzen. Diese Regelung ist gerechtfertigt, da die Ausschussmitglieder im Interesse der von ihnen vertretenen Gruppe tätig werden. Da § 86 Verwaltungsverfahrensgesetz nicht für anwendbar erklärt wird, ist eine Abberufung aus den dort genannten Gründen nicht möglich. Dies würde mit der Weisungsfreiheit der Mitglieder des Ausschusses nach § 12 Abs. 1 Satz 2 kollidieren.

Absatz 2:

Absatz 2 stellt Mindestanforderungen an die fachliche Kompetenz der Ausschussmitglieder, damit sie ihre Aufgaben sachgerecht erfüllen können. Die Fachkenntnis der Ausschussmitglieder wirkt sich unmittelbar auf die Qualität der Arbeit des Ausschusses aus. Mittelbar wird dadurch das Vertrauen der Verbraucherinnen und Verbraucher in das Datenschutzauditsiegel gestärkt.

Absatz 3:

Absatz 3 regelt, dass die Berufung der Mitglieder des Datenschutzauditausschusses und ihrer Stellvertreter durch das Bundesministerium des Innern erfolgt. Die Berufung erfolgt für die in Absatz 1 Satz 1 Nummer 3 bis 6 genannten Gruppen auf Vorschlag der jeweiligen Gruppe und im Einvernehmen mit der jeweiligen Gruppe. Für die Berufung eines Mitglieds muss also nicht das Einvernehmen mit allen im Datenschutzauditausschuss vertretenen Gruppen herbeigeführt werden. Dies birgt die Gefahr, dass mangels Einvernehmens der Ausschuss nicht besetzt werden kann und berührt die Unabhängigkeit der betroffenen Mitglieder. Das Vorschlagsrecht für die zu berufenden Mitglieder des Datenschutzauditausschusses liegt bei den Bundesdachverbänden der Wirtschaft, den Aufsichtsbehörden der Länder für den Datenschutz im nicht-öffentlichen Bereich, dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sowie den für den Da-

tenschutz zuständigen obersten Landesbehörden. Als Bundesdachverbände der Wirtschaft kommen in Betracht: der Bundesverband der Deutschen Industrie, die Bundesvereinigung der Deutschen Arbeitgeberverbände, der Deutsche Industrie- und Handelstag, der Zentralverband des Deutschen Handwerks und der Bundesverband freier Berufe. Für die Nummer 1 besitzt das Bundesministerium des Innern als für den allgemeinen Datenschutz zuständiges Bundesressort das Vorschlagsrecht. Dies gilt auch hinsichtlich der Nummer 2 für das Bundesamt für Sicherheit in der Informationstechnik aus seinem Geschäftsbereich.

Die Berufungsdauer von drei Jahren soll eine personelle Stabilität für den Datenschutzauditausschuss erreichen. Eine erneute Berufung wird nicht ausgeschlossen.

Zu § 13 (Geschäftsordnung, Vorsitz und Beschlussfassung des Datenschutzauditausschusses)

Die Vorschrift regelt Grundsätze der Willensbildung des Datenschutzauditausschusses.

Absatz 1:

Absatz 1 enthält einen Genehmigungsvorbehalt für das Bundesministerium des Innern im Hinblick auf die Geschäftsordnung des Datenschutzauditausschusses, der Teil der Rechtsaufsicht ist. Die Geschäftsordnung könnte z.B. das Ausscheiden eines Mitglieds vor Ablauf der Berufungsperiode, die Rolle des Stellvertreters und des Vorsitzenden, den Sitzungsablauf und die -häufigkeit, die Sitzungsteilnahme von Externen, die Niederschrift, die Einsetzung von Arbeitsgruppen und die Tätigkeit der Geschäftsstelle regeln.

Absatz 2:

Absatz 2 stellt sicher, dass im Vorstand alle relevanten Gruppen vertreten sind. Näheres zur Wahl regelt die Geschäftsordnung. Die Wahl bedarf daher als Angelegenheit der Geschäftsordnung der Mehrheit der gesetzlichen Mitgliederzahl.

Absatz 3:

Absatz 3 regelt das Beschlussverfahren des Datenschutzauditausschusses. Im Interesse der Praktikabilität ist die erforderliche Mehrheit je nach Beratungsgegenstand unterschiedlich. Nummer 1 sieht eine Mehrheit von zwei Dritteln (zwölf Stimmen) der Mitglieder bei der Verabschiedung von Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit vor. Auf diese Weise wird verhindert, dass eine Gruppe den Datenschutzauditausschuss majorisiert. Die Sperrminorität beträgt sieben Stimmen, so dass eine Gruppe den Datenschutzauditausschuss auch nicht blockieren kann. Nummer 2 verlangt die Mehrheit der gesetzlichen Mitgliederzahl in Geschäftsordnungsangelegenheiten, damit nicht Zufallsmehrheiten zur Benachteiligung einzelner Gruppen führen.

Zu § 14 (Geschäftsstelle)

Die Vorschrift schafft die personellen und organisatorischen Voraussetzungen für die Arbeitsfähigkeit des Datenschutzauditausschusses. Da der Datenschutzauditausschuss keine eigene Rechtspersönlichkeit besitzt und somit kein Personal einstellen und keine organisatorische Infrastruktur schaffen kann, muss eine Geschäftsstelle zur Verfügung gestellt werden. Näheres obliegt der Ausgestaltung durch die Geschäftsordnung. Einrichtung und Unterhaltung der Geschäftsstelle können nicht durch eine im Datenschutzauditausschuss vertretene Gruppe, sondern müssen durch den Bund erfolgen.

Zu § 15 (Rechtsaufsicht)

Absatz 1:

Absatz 1 unterstellt den Datenschutzauditausschuss der Aufsicht des Bundesministeriums des Innern und beschränkt die Aufsicht auf die Rechtmäßigkeit der Ausschusstätigkeit. Diese Beschränkung ergibt sich aus den Selbstverwaltungselementen, die den Datenschutzauditausschuss kennzeichnen.

Absätze 2 bis 4:

Die Absätze 2 bis 4 regeln die herkömmlichen Instrumente körperschaftlicher Rechtsaufsicht. Sie orientieren sich insbesondere an den bewährten Regelungen zum Umweltgutachterausschuss (§ 27 des Umweltauditgesetzes), die zurückgehen auf Instrumente der Kommunalaufsicht und der Aufsicht über die Handwerkskammern (§§ 105, 115 der Handwerksordnung). Absatz 4 ist der Regelung des § 115 Abs. 2 der Handwerksordnung nachgebildet. Das Auflösungsrecht greift als ultima ratio ein, wenn der Datenschutzauditausschuss seine gesetzlichen Aufgaben nach § 16 nicht mehr erfüllen kann, weil sich z.B. die im Datenschutzauditausschuss vertretenen Gruppen durch Ausübung ihrer Sperrminoritäten gegenseitig blockieren. In der Praxis dürfte allein das Bestehen des Auflösungsrechts ausreichen, um eine solche Entwicklung zu verhindern.

Zu § 16 (Verordnungsermächtigungen)

Absatz 1:

Absatz 1 greift die Möglichkeit der Länder auf, die Erfüllung ihrer hoheitlichen Aufgaben Kontrollstellen durch Rechtsverordnung zu übertragen oder sie daran zu beteiligen. Damit soll den Ländern ein verfahrenstechnisch möglichst einfacher Weg geboten werden, zur Wahrnehmung ihrer Aufgaben im Zusammenhang mit der Durchführung des Gesetzes die Beleihung oder Mitwirkung Privater vorzusehen.

Absatz 2:

Absatz 2 ist eine notwendige Folge der Regelung in § 2 Abs. 1 Satz 2 und eröffnet die zu Absatz 1 dargestellten Möglichkeiten der Übertragung und Beteiligung auf Kontrollstellen auch dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Ermächtigt wird das Bundesministerium des Innern, bei dem der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit nach § 22 Abs. 5 Satz 1 des Bundesdatenschutzgesetzes eingerichtet ist, im Einvernehmen mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit ohne Zustimmung des Bundesrates.

Absatz 3:

Die Vorschrift sieht in Absatz 3 Nr. 1 die erforderliche Ermächtigung des Bundesministeriums des Innern vor, um bei Bedarf im Wege einer Rechtsverordnung mit Zustimmung des Bundesrates Einzelheiten der Verwendung des Datenschutzauditsiegels vorzusehen. Nummer 2 eröffnet die Möglichkeit, erforderlichenfalls das Verfahren der Zulassung der Kontrollstellen sowie das Verfahren für deren Entziehung durch Rechtsverordnung mit Zustimmung des Bundesrates näher zu regeln. Nummer 3 sieht die erforderliche Ermächtigung vor, um im Wege einer Rechtsverordnung mit Zustimmung des Bundesrates Mindestkontrollanforderungen und im Rahmen des Kontrollverfahrens vorgesehene Vorkehrungen festzulegen. Nummer 4 sieht vor, die Gestaltung des Datenschutzauditsiegels und Nummer 5 die Anzeige der Verwendung des Datenschutzauditsiegels an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit näher zu regeln.

Die Rechtsverordnung nach Nummer 1 soll neben der Verwendung, insbesondere die Art und den Ort der Anbringung des Datenschutzauditsiegels regeln. Die Rechtsverordnung nach Nummer 2 soll insbesondere die Voraussetzungen für die Zulassung und die Entziehung der Zulassung näher ausführen. Die Rechtsverordnung nach Nummer 3 soll Einzelheiten zu dem Standardkontrollverfahren der Kontrollstellen regeln, insbesondere zur

Häufigkeit der Kontrollen und zur Intensität der Überprüfung sowie die Pflichten der kontrollierten Stellen, um die Wirksamkeit der Kontrollen zu gewährleisten. Die Rechtsverordnung nach Nummer 4 soll neben einer genauen Beschreibung des Datenschutzauditsiegels in allen Wort- und Grafikbestandteilen insbesondere regeln, wie stark das Datenschutzauditsiegel abgewandelt werden darf (maximale Vergrößerung oder Verkleinerung, Zulässigkeit von Zusätzen) und welche Kombinationsmöglichkeit mit anderen Zertifikaten und Kennzeichnungen bestehen. Der Bundesadler findet keine Verwendung, da die Voraussetzungen nach dem Erlass über die Dienstsiegel vom 20. Januar 1950 (BGBl. S. 26) nicht vorliegen. Die Rechtsverordnung nach Nummer 5 soll insbesondere die verpflichtenden Angaben für die Anzeige in Gestalt eines Formblattes aufführen.

Zu § 17 (Bußgeldvorschrift)

Die Vorschrift enthält die erforderlichen Bußgeldtatbestände, insbesondere bei vorsätzlich oder fahrlässig unbefugter Verwendung des Datenschutzauditsiegels oder unzureichender Anzeige der Verwendung gegenüber dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit durch Unternehmen.

Für Kontrollstellen soll es einen Bußgeldtatbestand darstellen, einen Kontrollbericht nicht, nicht richtig oder vollständig zu erstellen sowie nicht richtig oder rechtzeitig über festgestellte Unregelmäßigkeiten oder Verstöße zu unterrichten, da eine unterlassene oder verspätete Meldung zu unvertretbaren Lücken im Kontroll- und Überwachungssystem führen kann. Ferner soll die unterlassene rechtzeitige Mitteilung einer Kontrollstelle an die von ihr kontrollierten Unternehmen die zuständigen Behörden und den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit über die voraussichtliche Beendigung der Kontrolltätigkeit als Ordnungswidrigkeit geahndet werden können, da den kontrollierten Unternehmen infolge unterlassener oder verspäteter Mitteilung erhebliche Nachteile entstehen können.

Einen Bußgeldtatbestand sowohl für kontrollierte Unternehmen als auch Kontrollstellen soll es darstellen, jeweils im Rahmen der Überwachung durch Kontrollstellen und zuständige Behörden Auskünfte unzureichend zu erteilen, Maßnahmen nicht zu dulden, Unterlagen nicht vorzulegen oder in anderer Weise die erforderliche Hilfe zu versagen.

Der Strafrahmen entspricht demjenigen nach § 43 Abs. 3 in Verbindung mit Abs. 2 des Bundesdatenschutzgesetzes.

Zu § 18 (Strafvorschrift)

Die Vorschrift stellt das unbefugte Verwenden des Datenschutzauditsiegels in Bereicherungs- oder Schädigungsabsicht unter Strafe. Der Strafrahmen entspricht demjenigen nach § 44 Abs. 1 des Bundesdatenschutzgesetzes.

Zu § 19 (Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten)

Die Vorschrift sieht, abweichend von dem geplanten § 44a des Bundesdatenschutzgesetzes eine Privilegierung von solchen Unternehmen vor, bei denen die unrechtmäßige Kenntniserlangung durch Dritte sich auf Daten bezieht, für deren Erhebung, Verarbeitung oder Nutzung ein Datenschutzkonzept gilt, für das ein Datenschutzauditsiegel verwendet werden darf oder die bei der verantwortlichen Stelle unmittelbar zuvor mittels einer technischen Einrichtung verarbeitet wurden, für die ein Datenschutzauditsiegel verwendet werden darf. In diesem Fall unterliegt das Unternehmen nach § 1 Satz 2 Nr. 4 einer regelmäßigen Kontrolle durch Kontrollstellen. Die Kontrolle der Behebung des Verstoßes, der zur unrechtmäßigen Kenntniserlangung geführt hat, ist bei diesen Unternehmen, anders als bei sonstigen Unternehmen in Bezug auf die Aufsichtsbehörden, sichergestellt. Daher ist es gerechtfertigt, die Benachrichtigung auf die Kontrollstelle zu begrenzen.

Zu § 20 (Einziehung)

Die Vorschrift enthält die übliche nebenstrafrechtliche Regelung.

Zu Artikel 3

Die Vorschrift regelt das Inkrafttreten des Gesetzes.

Artikel 1 des Gesetzes soll am … in Kraft treten. Aufgrund der Übergangsvorschrift in Artikel 3 verbleiben den betroffenen verantwortlichen Stellen damit … Monate, ihre Datenbestände den neuen Anforderungen anzupassen und Daten nach der neuen Fassung des § 28 des Bundesdatenschutzgesetzes zu erheben.

Artikel 2 des Gesetzes soll am … in Kraft treten, damit sich der Datenschutzauditausschuss frühzeitig konstituieren kann und mit dem Erlass der Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit die Grundlage für die Verwendung des Datenschutzauditsiegels schaffen kann.