Gesetzentwurf

der Bundesregierung

Entwurf eines

Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften

A. Problem und Ziel

Den Aufwendungen von Unternehmen für einen über das gesetzlich vorgeschriebene Datenschutzniveau hinausgehenden Datenschutz soll ein adäquater wirtschaftlicher Mehrwert gegenüber stehen. Ein freiwilliges, gesetzlich geregeltes Datenschutzaudit mit der Vergabe eines Datenschutzauditsiegels verbindet Förderung des Datenschutzes und Wirtschaftsförderung miteinander. Zugleich soll die Ankündigung eines Datenschutzauditgesetzes in § 9a Satz 2 des Bundesdatenschutzgesetzes erfüllt werden.

In der jüngeren Vergangenheit sind zunehmend Fälle des rechtswidrigen Handels mit personenbezogenen Daten bekannt geworden Die Herkunft der Daten ist größtenteils nicht nachvollziehbar. Der Erlaubnistatbestand des § 28 Absatz 3 Satz 1 Nummer 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 weitläufig zum Erwerb oder zur Nutzung angeboten werden, ohne in jedem Fall die in der Vorschrift angelegten Anforderungen zu beachten. Zudem hat sich das Verhältnis der Bürgerinnen und Bürger zu Werbung, Markt- und Meinungsforschung seit dem Bestehen der Vorschrift gewandelt: Die Betroffenen möchten über die Verwendung personenbezogener Daten für diese Zwecke selbst entscheiden können.

B. Lösung

Unternehmen wird die Möglichkeit eröffnet, sich freiwillig einem gesetzlich geregelten unbürokratischen Datenschutzaudit zu unterziehen und Datenschutzkonzepte und technische Einrichtungen mit einem Datenschutzsiegel zu kennzeichnen. Dabei kontrollieren zugelassene Kontrollstellen in regelmäßigen Abständen, ob die gekennzeichneten Konzepte und Einrichtungen von einem mit Experten aus Wirtschaft und Verwaltung besetzten Ausschuss erlassene Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit erfüllen. Unternehmen, die sich dem Kontrollverfahren unterwerfen, dürfen im Rechts- und Geschäftsverkehr ein Datenschutzauditsiegel verwenden und hiermit werben.

Die Erlaubnis zur Verwendung personenbezogener Daten zum Zwecke der Werbung, Markt- und Meinungsforschung ohne Einwilligung der Betroffenen wird beschränkt auf Werbung für eigene Angebote oder die eigene Markt- oder Meinungsforschung der Stellen, die im Rahmen einer Vertragsbeziehung mit dem Betroffenen Daten über ihn erhalten haben, sowie bestimmter Empfänger steuerbegünstigter Spendenwerbung. Die Verwendung personenbezogener Daten für Zwecke des Adresshandels sowie für fremde Werbezwecke oder Markt- oder Meinungsforschung soll nur mit Einwilligung der Betroffenen

möglich sein. Zudem sollen marktbeherrschende Unternehmen die Einwilligung nicht durch Kopplung mit dem Vertragsschluss erzwingen dürfen.

C. Alternativen

Keine.

D. Finanzielle Auswirkungen auf die öffentlichen Haushalte

1. Haushaltsausgaben ohne Vollzugsaufwand

Keine.

2. Vollzugsaufwand

Das Gesetz bewirkt Vollzugsaufwand bei den Ländern und in einem Teilbereich beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit im Rahmen der Durchführung des Gesetzes und der Überwachung der zugelassenen Kontrollstellen. Die Kosten für die einzelnen Auditverfahren können durch Kostenordnungen auf die Antragsteller abgewälzt werden. Weiterer Vollzugsaufwand entsteht beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit durch die Zulassung der Kontrollstellen und ggf. die Entziehung der Zulassung sowie das Führen eines Verzeichnisses der Kontrollstellen und der in das Kontrollsystem einbezogenen Datenschutzkonzepte und technischen Einrichtungen. Ferner entsteht Vollzugsaufwand durch die Bildung eines Datenschutzauditausschusses mit Vertretern aus Bund, Ländern und der Wirtschaft nebst Geschäftsstelle beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Hierfür können in Abhängigkeit von der Zahl der Kontrollstellen bis zu 15 zusätzliche Stellen sowie jährlich Haushaltsmittel in Höhe von rd. 1,2 Mio. Euro für Personal- und Sachausgaben benötigt werden. Über die Ausbringung und Finanzierung dieser Personal- und Sachausgaben ist im Haushaltsaufstellungsverfahren 2010 zu entscheiden.

E. Sonstige Kosten

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

Im Rahmen des Datenschutzauditgesetzes können Kosten für die Wirtschaft nach Maßgabe von ggf. von den Ländern und dem Bund zu erlassenden Kostenordnungen entstehen, durch die die Kosten für die einzelnen Auditverfahren auf die Unternehmen abgewälzt werden können. Da ein Datenschutzaudit freiwillig ist, können es die Unternehmen von einer Wirtschaftlichkeitsbetrachtung abhängig machen, ob sie sich einem Audit mit der damit einhergehenden Kostenfolge unterziehen.

F. Bürokratiekosten

Für die Wirtschaft werden 15 Informationspflichten neu eingeführt und eine Informationspflicht geändert. Es wird keine Informationspflicht abgeschafft. Die Summe der zu erwartenden Belastungen für die Wirtschaft beträgt 10,14 Mio. Euro.

Für die Bürgerinnen und Bürger wird keine Informationspflicht neu eingeführt, geändert oder abgeschafft.

Für die Verwaltung werden zwölf Informationspflichten neu eingeführt und keine Informationspflicht geändert oder abgeschafft.

Entwurf eines
Gesetzes zur Regelung des Datenschutzaudits
und zur Änderung datenschutzrechtlicher Vorschriften

Vom [Datum der Ausfertigung]

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Datenschutzauditgesetz
(DSAG)[1]

Inhaltsübersicht

[1] Die Verpflichtungen aus der Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 204 vom 21.7.1998, S. 37), die zuletzt durch die Richtlinie 2006/96/EG vom 20. November 2006 (ABl. L 363 vom 20.12.2006, S. 81) geändert worden ist, sind beachtet worden.

§ 1

Datenschutzaudit

Nach Maßgabe dieses Gesetzes können

1. verantwortliche Stellen ihr Datenschutzkonzept und

2. Anbieter von Datenverarbeitungsanlagen und -programmen (informationstechnischen Einrichtungen) die angebotenen informationstechnischen Einrichtungen

kontrollieren lassen, sofern sie nichtöffentliche Stellen im Sinne des § 2 Absatz 4 des Bundesdatenschutzgesetzes sind. Sie dürfen ihr Datenschutzkonzept oder eine angebotene informationstechnische Einrichtung mit einem Datenschutzauditsiegel kennzeichnen, wenn

1. bei der Datenverarbeitung, für die das Datenschutzkonzept oder die informationstechnische Einrichtung vorgesehen ist, die Vorschriften zum Schutz personenbezogener Daten eingehalten werden,

2. die für das Datenschutzkonzept oder die informationstechnische Einrichtung geltenden Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit nach § 11 Absatz 1 erfüllt werden,

3. als Anbieter mit Sitz im Inland die Vorschriften des Bundesdatenschutzgesetzes über die organisatorische Stellung des Beauftragten für den Datenschutz eingehalten werden und

4. dies nach § 3 kontrolliert wird.

Nichtöffentliche Stellen im Sinne dieses Gesetzes sind auch die in § 27 Absatz 1 Satz 1 Nummer 2 des Bundesdatenschutzgesetzes genannten Stellen.

§ 2

Zuständigkeit

(1) Die Durchführung dieses Gesetzes und der auf Grund dieses Gesetzes erlassenen Rechtsverordnungen obliegt den nach Landesrecht zuständigen Behörden, soweit nachstehend nichts anderes bestimmt ist. Soweit für die geschäftsmäßige Erbringung von Post- oder Telekommunikationsdiensten Daten zu natürlichen oder juristischen Personen erhoben, verarbeitet oder genutzt werden, ist zuständige Behörde der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (Bundesbeauftragter).

(2) Der Bundesbeauftragte ist zuständig für die Zulassung der Kontrollstellen, die Entziehung der Zulassung und die Vergabe der Kennnummern an die Kontrollstellen.

§ 3

Kontrollen

Vorbehaltlich einer Rechtsverordnung nach § 16 Absatz 1 Satz 1 Nummer 1 oder § 16 Absatz 2 Satz 1 Nummer 1 werden die Kontrollen nach § 1 Satz 2 Nummer 4 von zugelassenen Kontrollstellen durchgeführt, soweit die Aufgabenwahrnehmung nicht mit der Durchführung eines Verwaltungsverfahrens verbunden ist. Der Beauftragte für den Datenschutz nach § 4f Absatz 1 Satz 1 des Bundesdatenschutzgesetzes ist in die Durchführung der Kontrollen einzubeziehen. Art und Häufigkeit der Kontrollen richten sich nach dem Risiko des Auftretens von Verstößen gegen dieses Gesetz, die auf Grund dieses Gesetzes erlassenen Rechtsverordnungen oder die für das Datenschutzkonzept oder die informationstechnische Einrichtung geltenden Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit nach § 11 Absatz 1. Jede nichtöffentliche Stelle, die eine Anzeige nach § 9 Absatz 1 Satz 1 erstattet hat, wird, sobald der ordnungsgemäße Geschäftsbetrieb der Kontrollstelle es ermöglicht, erstmalig und sodann spätestens innerhalb von zwölf Monaten nach dieser Kontrolle erneut kontrolliert. Danach wird die nichtöffentliche Stelle spätestens alle 18 Monate kontrolliert.

§ 4

Zulassung der Kontrollstelle und Entziehung der Zulassung

(1) Eine Kontrollstelle ist auf Antrag zuzulassen, wenn

1. ihr Leitungspersonal und die für Kontrollen verantwortlichen Beschäftigten über die erforderliche Zuverlässigkeit, Unabhängigkeit und fachliche Eignung verfügen,

2. die Kontrollstelle akkreditiert ist,

3. die für die Zulassung erhobenen Gebühren entrichtet worden sind und

4. die Kontrollstelle ihren Sitz oder eine Niederlassung im Bundesgebiet hat.

Mit der Zulassung ist der Kontrollstelle eine Kennnummer zuzuteilen.

(2) Die Zulassung wird für das gesamte Bundesgebiet erteilt. Auf Antrag kann die Zulassung auf einzelne Länder beschränkt werden.

(3) Die Zulassung kann mit Befristungen, Bedingungen oder einem Vorbehalt des Widerrufs erlassen oder mit Auflagen verbunden werden, soweit die Funktionsfähigkeit des Kontrollsystems oder Belange des Datenschutzes hinsichtlich der Voraussetzungen nach Absatz 1 Nummer 1 oder Nummer 2 dies erfordern. Unter denselben Voraussetzungen ist die nachträgliche Aufnahme und die Änderung von Auflagen zulässig.

(4) Einer Kontrollstelle wird die Zulassung entzogen, wenn die Kontrollstelle

1. den Anforderungen nach Absatz 1 Satz 1 Nummer 1, Nummer 2 oder Nummer 4 nicht mehr genügt,

2. ihren Verpflichtungen nach diesem Gesetz, insbesondere nach § 6 oder § 8 Absatz 3, oder nach einer aufgrund dieses Gesetzes erlassenen Rechtsverordnung in schwerwiegender Weise nicht nachkommt.

§ 5

Anforderungen an das Personal der Kontrollstelle

(1) Über die erforderliche Zuverlässigkeit verfügt, wer auf Grund seiner persönlichen Eigenschaften, seines Verhaltens und seiner Fähigkeiten die Gewähr für die ordnungsgemäße Erfüllung der ihm obliegenden Aufgaben bietet. Für die Zuverlässigkeit bietet in der Regel keine Gewähr, wer

1. ausweislich eines Führungszeugnisses für Behörden nach § 30 Absatz 5, § 31 des Bundeszentralregistergesetzes wegen Verletzung der Vorschriften des Strafrechts über den persönlichen Lebens- und Geheimbereich, über Eigentums- und Vermögensdelikte, Urkundenfälschung oder Insolvenzstraftaten mit einer Strafe oder wegen Verletzung gewerbe- oder arbeitsschutzrechtlicher Vorschriften mit einer Geldbuße in Höhe von mehr als fünfhundert Euro belegt worden ist,

2. wiederholt oder grob pflichtwidrig gegen dieses Gesetz, eine aufgrund dieses Gesetzes erlassene Rechtsverordnung oder Vorschriften über den Schutz personenbezogener Daten verstoßen hat oder wiederholt oder grob pflichtwidrig als Beauftragter für den Datenschutz seine Verpflichtungen verletzt hat,

3. infolge strafgerichtlicher Verurteilung die Fähigkeit zur Bekleidung öffentlicher Ämter verloren hat,

4. sich nicht in geordneten wirtschaftlichen Verhältnissen befindet, es sei denn, dass dadurch die Interessen der kontrollierten nichtöffentlichen Stelle oder Dritter nicht gefährdet sind, oder

5. aus gesundheitlichen Gründen nicht nur vorübergehend unfähig ist, die Kontrollen nach Maßgabe der nach § 16 Absatz 3 Nummer 3 zu erlassenden Rechtsverordnung ordnungsgemäß durchzuführen.

(2) Über die erforderliche Unabhängigkeit verfügt, wer bei der Übernahme, Vorbereitung und Durchführung der Kontrollen keiner persönlichen, wirtschaftlichen oder beruflichen Einflussnahme unterliegt, die geeignet ist, ein objektives Urteil zu beeinträchtigen. Für die Unabhängigkeit und Freiheit von Interessenkonflikten bietet in der Regel keine Gewähr, wer

1. neben seiner Tätigkeit für die Kontrollstelle Inhaber oder Angestellter einer nichtöffentlichen Stelle ist, auf die sich seine Kontrolltätigkeit bezieht,

2. als Leitungspersonal der Kontrollstelle eine Tätigkeit auf Grund eines Beamtenverhältnisses, Soldatenverhältnisses oder eines Anstellungsvertrages mit einer juristischen Person des öffentlichen Rechts, eine Tätigkeit auf Grund eines Richterverhältnisses, öffentlich-rechtlichen Dienstverhältnisses als Wahlbeamter auf Zeit oder eines öffentlich-rechtlichen Amtsverhältnisses ausübt, es sei denn, dass die übertragenen Aufgaben ehrenamtlich wahrgenommen werden,

3. Weisungen auf Grund vertraglicher oder sonstiger Beziehungen bei der Tätigkeit für die Kontrollstelle auch dann zu befolgen hat, wenn sie zu Handlungen gegen seine Überzeugung verpflichten,

4. organisatorisch, wirtschaftlich, kapitalmäßig oder personell mit Dritten verflochten ist, wenn nicht deren Einflussnahme auf die Wahrnehmung der Auf-

gaben für die Kontrollstelle, insbesondere durch Satzung, Gesellschaftsvertrag oder Anstellungsvertrag ausgeschlossen ist.

(3) Über die erforderliche fachliche Eignung verfügt, wer auf Grund seiner Ausbildung, beruflichen Bildung und praktischen Erfahrung zur ordnungsgemäßen Erfüllung der ihm obliegenden Aufgaben befähigt ist. Im Bereich Recht sind nachzuweisen:

1. der Abschluss eines Studiums der Rechtswissenschaft oder eines Studiums auf einem anderen Gebiet mit rechtswissenschaftlichen Inhalten, die den Umfang eines durchschnittlichen Nebenfachstudiums der Rechtswissenschaft nicht unterschreiten, an einer deutschen Hochschule oder ein gleichwertiger ausländischer Abschluss sowie eine dreijährige berufliche Tätigkeit mit dem Schwerpunkt auf dem Gebiet des Datenschutzrechts oder

2. eine Aus-, Fort- und Weiterbildung im Datenschutzrecht sowie eine mindestens fünfjährige berufliche Tätigkeit mit dem Schwerpunkt auf dem Gebiet des Datenschutzrechts.

Im Bereich Informationstechnik sind nachzuweisen:

1. der Abschluss eines Studiums der Informatik, der Wirtschaftsinformatik oder eines Studiums auf einem anderen Gebiet mit informationstechnischen Inhalten, die den Umfang eines durchschnittlichen Nebenfachstudiums der Informatik nicht unterschreiten, an einer deutschen Hochschule oder ein gleichwertiger ausländischer Abschluss sowie eine dreijährige berufliche Tätigkeit mit dem Schwerpunkt auf dem Gebiet der Informationstechnik oder

2. eine Aus-, Fort- und Weiterbildung auf dem Gebiet der Informationstechnik sowie eine mindestens fünfjährige berufliche Tätigkeit mit dem Schwerpunkt auf dem Gebiet der Informationstechnik.

Die berufliche Tätigkeit darf zum Zeitpunkt des Tätigwerdens für die Kontrollstelle nicht seit mehr als drei Jahren unterbrochen sein.

§ 6

Pflichten der Kontrollstelle

(1) Die Kontrollstelle hat ein Datenschutzkonzept oder eine informationstechnische Einrichtung gegen angemessene Vergütung in ihre Kontrollen einzubeziehen, soweit die nichtöffentliche Stelle die Einbeziehung verlangt und ihren Sitz oder eine Niederlassung in dem Land hat, in dem die Kontrollstelle zugelassen ist. Die zuständige Behörde kann auf Antrag der Kontrollstelle eine Ausnahme von der Verpflichtung nach Satz 1 zulassen, soweit

1. die Kontrollstelle wirksame Kontrollen nicht gewährleisten kann und

2. die Durchführung der Kontrollen durch eine andere Kontrollstelle sichergestellt ist.

(2) Die Kontrollstelle übermittelt der zuständigen Behörden jährlich bis zum 31. Januar ein Verzeichnis der nichtöffentlichen Stellen, die am 31. Dezember des Vorjahres ihrer Kontrolle unterstanden und legt bis zum 31. März jedes Jahres einen Bericht über ihre Tätigkeit im Vorjahr vor.

(3) Die Kontrollstellen erteilen einander die für eine ordnungsgemäße Durchführung dieses Gesetzes notwendigen Auskünfte. Stellt eine Kontrollstelle bei ihrer Tätigkeit Verstöße gegen § 1 Satz 2 Nummer 1 bis 3 fest, unterrichtet sie unverzüglich die zuständige Behörde. Soweit eine Kontrollstelle im Rahmen der von ihr durchgeführten Kontrollen Tatsachen feststellt, die einen hinreichenden Verdacht auf Verstöße der in Satz 2 genannten Art begründen, der eine nicht von der Kontrollstelle kontrollierte nichtöffentliche Stelle betrifft, teilt die Kontrollstelle die Tatsachen unverzüglich der Kontrollstelle mit, deren Kontrolle die betroffene nichtöffentliche Stelle untersteht.

(4) Die Kontrollstelle unterrichtet die von ihr kontrollierten nichtöffentlichen Stellen, die nach Landesrecht für die Sitze oder Niederlassungen der nichtöffentlichen Stellen zuständigen Behörden sowie den Bundesbeauftragten,

1. spätestens drei Monate vor der beabsichtigten Einstellung ihrer Tätigkeit,

2. im Falle eines Antrags auf Eröffnung eines Insolvenzverfahrens unverzüglich.

Die Kontrollstelle darf, soweit insolvenzrechtliche Vorschriften nicht entgegenstehen, ihre Tätigkeit erst einstellen, wenn die Kontrolle der von ihr kontrollierten nichtöffentlichen Stellen durch eine andere Kontrollstelle sichergestellt ist.

§ 7

Pflichten der zuständigen Behörde

(1) Die Kontrollstelle wird von der zuständigen Behörde des Landes, in dem die Kontrollstelle ihre Tätigkeit ausübt, überwacht, indem die zuständige Behörde bei Bedarf Überprüfungen der Kontrollstelle veranlasst. Auf Ersuchen erteilen die zuständigen Behörden einander die zur Überwachung der Kontrollstellen erforderlichen Auskünfte. Stellt die zuständige Behörde Tatsachen fest, die die Entziehung der Zulassung rechtfertigen oder die Aufnahme oder Änderung von Auflagen zur Zulassung erforderlich machen können, hat sie

1. wenn der Ort der zu beanstandenden Kontrolltätigkeit und der Sitz oder die Niederlassung der Kontrollstelle in demselben Land liegen, beim Bundesbeauftragten unter Mitteilung dieser Tatsachen die Entziehung der Zulassung oder die Aufnahme oder Änderung von Auflagen anzuregen oder,

2. wenn der Ort der zu beanstandenden Kontrolltätigkeit und der Sitz oder die Niederlassung der Kontrollstelle in verschiedenen Ländern liegen, der zuständigen Behörde des Landes, in dem der Sitz oder die Niederlassung der Kontrollstelle liegt, die Tatsachen mitzuteilen.

Erhält die zuständige Behörde des Landes, in dem der Sitz oder die Niederlassung der Kontrollstelle liegt, Kenntnis von Tatsachen nach Satz 3 Nummer 2, regt sie beim Bundesbeauftragten unter Mitteilung dieser Tatsachen an, ein Verfahren zur Entziehung der Zulassung oder zur Aufnahme oder Änderung von Auflagen einzuleiten. Im Rahmen des § 2 Absatz 1 Satz 2 wird die Tätigkeit einer Kontrollstelle nach Satz 1 durch den Bundesbeauftragten überwacht.

(2) Im Falle des § 6 Absatz 3 Satz 2 kann die zuständige Behörde anordnen, dass von dem Verstoß betroffene Datenschutzkonzepte oder informationstechnische Einrichtungen nicht mit dem Datenschutzauditsiegel gekennzeichnet werden dürfen, wenn dies in einem angemessenen Verhältnis zur Bedeutung der Vorschrift, gegen die verstoßen wurde, sowie zu Art und Umständen des Verstoßes steht. Im Falle eines schwerwiegen-

den Verstoßes oder eines Verstoßes mit Langzeitwirkung kann die zuständige Behörde der nichtöffentlichen Stelle die Kennzeichnung für einen bestimmten Zeitraum untersagen.

§ 8

Überwachung

(1) Die nichtöffentlichen Stellen und die Kontrollstellen haben den zuständigen Behörden auf Verlangen die zur Durchführung der den zuständigen Behörden durch dieses Gesetz oder auf Grund dieses Gesetzes übertragenen Aufgaben erforderlichen Auskünfte zu erteilen.

(2) Die von der zuständigen Behörde beauftragten Personen dürfen Betriebsgrundstücke sowie Geschäfts- oder Betriebsräume der Auskunftspflichtigen während der Geschäfts- oder Betriebszeit betreten und dort Besichtigungen vornehmen und geschäftliche Unterlagen einsehen und prüfen, soweit dies zur Durchführung ihrer Aufgaben erforderlich ist.

(3) Auskunftspflichtige haben die Maßnahmen nach Absatz 2 zu dulden, die zu besichtigenden Bereiche selbst oder durch andere so zu bezeichnen, dass die Besichtigung ordnungsgemäß vorgenommen werden kann, selbst oder durch andere die erforderliche Hilfe bei Besichtigungen zu leisten sowie die geschäftlichen Unterlagen zur Einsichtnahme und Prüfung vorzulegen.

(4) Auskunftspflichtige können die Auskunft auf solche Fragen verweigern, deren Beantwortung sie oder einen der in § 383 Absatz 1 Nummer 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Auskunftspflichtige sind darauf hinzuweisen.

(5) Die Absätze 1 bis 4 gelten entsprechend für die Kontrollen der nichtöffentlichen Stellen durch die Kontrollstellen.

§ 9

Datenschutzauditsiegel, Verzeichnisse

(1) Wer ein Datenschutzkonzept oder eine informationstechnische Einrichtung mit dem Datenschutzauditsiegel kennzeichnen will, hat dies dem Bundesbeauftragten vor der erstmaligen Verwendung des Siegels anzuzeigen. Der Bundesbeauftragte hat ein Verzeichnis der angezeigten Datenschutzkonzepte sowie informationstechnischen Einrichtungen mit den Angaben nach Satz 3 zu führen und zum Zwecke der Information der zuständigen Behörden und der Betroffenen auf seiner Internetseite sowie im elektronischen Bundesanzeiger zu veröffentlichen. Das Verzeichnis muss folgende Angaben enthalten:

1. den Namen und die Anschrift oder die der nichtöffentlichen Stelle durch die Kontrollstelle zugeordnete alphanumerische Identifikationsnummer,

2. den Namen und die Anschrift oder die Kennnummer der Kontrollstelle,

3. das angezeigte Datenschutzkonzept sowie die informationstechnische Einrichtung.

Weitere Angaben darf das Verzeichnis nicht enthalten.

(2) Der Bundesbeauftragte hat ein Verzeichnis der zugelassenen Kontrollstellen mit den Angaben nach Satz 2 zu führen und zum Zwecke der Information der zuständigen Behörden und der Betroffenen auf seiner Internetseite sowie im elektronischen Bundesanzeiger zu veröffentlichen. Das Verzeichnis enthält die Namen, Anschriften und Kennnummern der zugelassenen Kontrollstellen. Weitere Angaben darf es nicht enthalten.

§ 10

Gebühren und Auslagen

(1) Für Amtshandlungen nach § 2 Absatz 1 Satz 2 und Absatz 2 sowie § 9 Absatz 1 und 2 können zur Deckung des Verwaltungsaufwandes Gebühren und Auslagen erhoben werden. Das Bundesministerium des Innern wird ermächtigt, im Einvernehmen mit dem Bundesministerium der Finanzen durch Rechtsverordnung ohne Zustimmung des Bundesrates die gebührenpflichtigen Tatbestände, die Gebührensätze sowie die Auslagenerstattung zu bestimmen und dabei feste Sätze oder Rahmensätze vorzusehen. In der Rechtsverordnung kann die Erstattung von Auslagen abweichend vom Verwaltungskostengesetz geregelt werden.

(2) Für Amtshandlungen der zuständigen Behörden nach § 7 Absatz 1 Satz 1 und Absatz 2 können Gebühren und Auslagen nach Maßgabe des Landesrechts erhoben werden.

§ 11

Datenschutzauditausschuss

(1) Beim Bundesbeauftragten wird ein Datenschutzauditausschuss gebildet. Er erlässt Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit, insbesondere durch

1. Transparenz der Datenerhebung, -verarbeitung und -nutzung,
2. Datenvermeidung und Datensparsamkeit nach § 3a des Bundesdatenschutzgesetzes,
3. die Stärkung der organisatorischen Stellung des Beauftragten für den Datenschutz nach § 4f Absatz 1 Satz 1 des Bundesdatenschutzgesetzes,
4. technische und organisatorische Maßnahmen nach § 9 des Bundesdatenschutzgesetzes.

Der Bundesbeauftragte veröffentlicht die Richtlinien auf seiner Internetseite und im elektronischen Bundesanzeiger.

(2) Der Datenschutzauditausschuss unterrichtet die Öffentlichkeit jährlich in einem Bericht über seine Tätigkeit und Erfahrungen, insbesondere über Praktikabilität und erforderliche Änderungen erlassener Richtlinien sowie den Bedarf für neue Richtlinien.

§ 12

Mitglieder des Datenschutzauditausschusses

(1) Mitglieder des Datenschutzauditausschusses sind

1. zwei Vertreter der Verwaltung des Bundes,
2. zwei Vertreter des Bundesamtes für Sicherheit in der Informationstechnik,
3. zwei Vertreter des Bundesbeauftragten,
4. zwei Vertreter der Verwaltung der Länder,
5. vier Vertreter von Aufsichtsbehörden der Länder für den Datenschutz im nichtöffentlichen Bereich,
6. sechs Vertreter von Unternehmen oder ihren Verbänden.

Sie unterliegen keinen Weisungen und sind ehrenamtlich tätig. Die §§ 83 und 84 des Verwaltungsverfahrensgesetzes sind anzuwenden.

(2) Die Mitglieder des Datenschutzauditausschusses müssen über gründliche Fachkenntnisse und mindestens dreijährige praktische Erfahrungen auf dem Gebiet des Datenschutzes verfügen.

(3) Das Bundesministerium des Innern beruft die Mitglieder des Datenschutzauditausschusses und für jedes Mitglied einen Stellvertreter für die Dauer von drei Jahren, die Mitglieder nach Absatz 1 Satz 1 Nummer 3 bis 6 auf Vorschlag und jeweils im Einvernehmen mit dem Bundesbeauftragten, den für den Datenschutz zuständigen obersten Landesbehörden, den Aufsichtsbehörden nach § 38 des Bundesdatenschutzgesetzes sowie den Bundesdachverbänden der Wirtschaft.

(4) Zu Sitzungen ist ein Vertreter der Bundesnetzagentur mit beratender Stimme hinzuzuziehen, soweit Gegenstand der Sitzung eine Richtlinie ist, die nichtöffentliche Stellen betrifft, die nach § 115 Absatz 4 Satz 1 des Telekommunikationsgesetzes oder § 42 Absatz 3 des Postgesetzes der Kontrolle des Bundesbeauftragten unterliegen.

§ 13

Geschäftsordnung, Vorsitz und Beschlussfassung des Datenschutzauditausschusses

(1) Der Datenschutzauditausschuss gibt sich eine Geschäftsordnung, die der Genehmigung durch das Bundesministerium des Innern bedarf.

(2) Der Datenschutzauditausschuss wählt den Vorsitzenden und zwei Stellvertreter aus seiner Mitte. Zu ihnen muss jeweils ein Vertreter der Unternehmen oder ihrer Organisationen, der Aufsichtsbehörden für den Datenschutz und der Verwaltung gehören.

(3) Der Datenschutzauditausschuss beschließt

1. in Angelegenheiten nach § 11 Absatz 1 Satz 2 mit der Mehrheit von zwei Dritteln der gesetzlichen Mitglieder und

2. in Angelegenheiten der Geschäftsordnung mit der Mehrheit der gesetzlichen Mitglieder.

§ 14

Geschäftsstelle des Datenschutzauditausschusses

Der Datenschutzauditausschuss wird bei der Durchführung seiner Aufgaben durch eine Geschäftsstelle unterstützt, die den Weisungen des Vorsitzenden des Datenschutzauditausschusses unterliegt.

§ 15

Rechtsaufsicht

(1) Der Datenschutzauditausschuss untersteht der Aufsicht des Bundesministeriums des Innern (Aufsichtsbehörde). Die Aufsicht erstreckt sich nur auf die Rechtmäßigkeit der Ausschusstätigkeit, insbesondere darauf, dass die Aufgabe nach § 11 Absatz 1 Satz 2 erfüllt wird.

(2) Die Aufsichtsbehörde kann an den Sitzungen des Datenschutzauditausschusses teilnehmen. Ihr ist auf Verlangen das Wort zu erteilen. Sie kann schriftliche Berichte und die Vorlage von Akten verlangen.

(3) Beschlüsse nach § 11 Absatz 1 Satz 2 bedürfen der Genehmigung durch die Aufsichtsbehörde. Die Aufsichtsbehörde kann rechtswidrige Beschlüsse des Datenschutzauditausschusses beanstanden und nach vorheriger Beanstandung aufheben. Wenn der Datenschutzauditausschuss Beschlüsse oder sonstige Handlungen unterlässt, die zur Erfüllung seiner gesetzlichen Aufgaben erforderlich sind, kann die Aufsichtsbehörde anordnen, dass innerhalb einer bestimmten Frist die erforderlichen Maßnahmen getroffen werden. Die Aufsichtsbehörde hat die geforderten Handlungen im Einzelnen zu bezeichnen. Sie kann ihre Anordnung selbst durchführen oder von einem anderen durchführen lassen, wenn die Anordnung vom Datenschutzauditausschuss nicht befolgt worden ist.

(4) Wenn die Aufsichtsmittel nach Absatz 3 nicht ausreichen, kann die Aufsichtsbehörde den Datenschutzauditausschuss auflösen. Sie hat nach Eintritt der Unanfechtbarkeit der Auflösungsanordnung unverzüglich neue Mitglieder gemäß § 12 Absatz 3 zu berufen. Sie braucht vorgeschlagene Personen nicht zu berücksichtigen, die dem aufgelösten Datenschutzauditausschuss angehört haben.

§ 16

Verordnungsermächtigungen

(1) Die Landesregierungen werden ermächtigt, durch Rechtsverordnung

1. zugelassene Kontrollstellen mit Aufgaben nach § 2 Absatz 1 Satz 1, ausgenommen die Aufgabe nach § 4, zu beleihen oder sie an der Erfüllung der Aufgaben zu beteiligen,

2. die Voraussetzungen und das Verfahren der Beleihung und der Beteiligung zu regeln

Die Landesregierungen können die Ermächtigung durch Rechtsverordnung ganz oder teilweise auf andere Behörden des Landes übertragen.

(2) Die Bundesregierung wird ermächtigt, nach Anhörung des Bundesbeauftragten durch Rechtsverordnung ohne Zustimmung des Bundesrates

1. zugelassene Kontrollstellen mit Aufgaben nach § 2 Absatz 1 Satz 2, ausgenommen die Aufgabe nach § 4, zu beleihen oder sie an der Erfüllung der Aufgaben zu beteiligen,

2. die Voraussetzungen und das Verfahren der Beleihung und der Beteiligung zu regeln.

(3) Das Bundesministerium des Innern wird ermächtigt, durch Rechtsverordnung mit Zustimmung des Bundesrates nähere Regelungen zu treffen über

1. die Einzelheiten der Verwendung des Datenschutzauditsiegels, um eine einheitliche Kennzeichnung und eindeutige Erkennbarkeit der Kennzeichnung der Datenschutzkonzepte und informationstechnischen Einrichtungen zu gewährleisten,

2. die Voraussetzungen und das Verfahren der Zulassung nach § 4 Absatz 1 bis 3 sowie die Voraussetzungen und das Verfahren der Entziehung der Zulassung nach § 4 Absatz 4, § 7 Absatz 1 Satz 3 und 4,

3. die Mindestanforderungen an die Kontrollen und die im Rahmen der Kontrollen vorgesehenen Vorkehrungen,

4. die Gestaltung des Datenschutzauditsiegels,

5. die Anzeige nach § 9 Absatz 1 Satz 1.

§ 17

Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer

1. entgegen § 6 Absatz 2 ein Verzeichnis nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt oder einen dort genannten Bericht nicht, nicht richtig oder nicht rechtzeitig vorlegt,

2. entgegen § 6 Absatz 3 Satz 2 oder Absatz 4 Satz 1 die zuständige Behörde, eine nichtöffentliche Stelle oder den Bundesbeauftragten nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet,

3. entgegen § 6 Absatz 3 Satz 3 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,

4. entgegen § 8 Absatz 1 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt,

5. entgegen § 8 Absatz 3 eine Maßnahme nicht duldet oder

6. entgegen § 9 Absatz 1 Satz 1, auch in Verbindung mit einer Rechtsverordnung nach § 16 Absatz 3 Nummer 5 eine Anzeige nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erstattet.

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig einer vollziehbaren Anordnung nach § 7 Absatz 2 Satz 2 zuwiderhandelt.

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

§ 18

Strafvorschriften

Wer eine in § 17 Absatz 2 bezeichnete vorsätzliche Handlung in der Absicht begeht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

§ 19

Einziehung

Ist eine Ordnungswidrigkeit nach § 17 Absatz 1 oder Absatz 2 oder eine Straftat nach § 18 begangen worden, können Gegenstände, auf die sich die Straftat oder die Ordnungswidrigkeit bezieht, und Gegenstände, die zu ihrer Begehung oder Vorbereitung gebraucht worden oder bestimmt gewesen sind, eingezogen werden. § 23 des Gesetzes über Ordnungswidrigkeiten und § 74a des Strafgesetzbuches sind anzuwenden.

§ 20

Übergangsvorschrift

§ 1 ist erst ab dem 1. Juli 2010 anzuwenden.

Artikel 2

Änderung des Bundesdatenschutzgesetzes

Das Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch das Gesetz vom …, wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:
   a) Nach der Angabe zu § 9 wird die Angabe „§ 9a Datenschutzaudit“ gestrichen.
   b) Die Angabe zu § 28 wie folgt gefasst:
      "§ 28 Datenerhebung und -speicherung für eigene Geschäftszwecke"
   c) Nach der Angabe zu § 42 wird folgende Angabe eingefügt:
      „§ 42a Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten“
   d) Nach der Angabe zu § 46 wird folgende Angabe eingefügt:
      „§ 47 Übergangsregelung“

2. Dem § 4f Absatz 3 werden folgende Sätze angefügt:
   „Ist der Beauftragte für den Datenschutz Arbeitnehmer einer nach Absatz 1 Satz 1 verpflichteten Stelle, für die das Kündigungsschutzgesetz gilt, so ist die Kündigung des Arbeitsverhältnisses unzulässig, es sei denn, dass Tatsachen vorliegen, welche die verantwortliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen. Nach der Abberufung als Beauftragter für den Datenschutz ist die Kündigung innerhalb eines Jahres nach der Beendigung der Bestellung unzulässig, es sei denn, dass die verantwortliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt ist. Zur Erhaltung der zur Erfüllung seiner Aufgaben erforderlichen Fachkunde hat die verantwortliche Stelle dem Beauftragten für den Datenschutz die Teilnahme an Fort- und Weiterbildungsveranstaltungen zu ermöglichen und deren Kosten zu übernehmen.“

3. § 9a wird aufgehoben.

4. In § 12 Absatz 4 wird die Angabe „§ 28 Abs. 1 und 3 Nr. 1“ durch die Angabe „§ 28 Absatz 1 und 2 Nummer 2 Buchstabe a“ ersetzt.

5. § 28 wird wie folgt geändert:
   a) Die Überschrift wird wie folgt gefasst:

„§ 28
Datenerhebung und -speicherung für eigene Geschäftszwecke“

b) In Absatz 1 Satz 1 Nummer 1 werden die Wörter "Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses" durch die Wörter "rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses" ersetzt.

c) Absatz 2 wird wie folgt gefasst:

„(2) Die Übermittlung oder Nutzung für einen anderen Zweck ist zulässig:

1. unter den Voraussetzungen des Absatzes 1 Satz 1 Nummer 2 oder Nummer 3,
2. soweit es erforderlich ist
   a) zur Wahrung berechtigter Interessen eines Dritten oder
   b) zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten

   und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat, oder
3. wenn es im Interesse einer Forschungseinrichtung zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.“

d) Absatz 3 wird wie folgt gefasst:

„(3) Die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke des Adresshandels, der Werbung oder der Markt- oder Meinungsforschung ist zulässig, soweit der Betroffene nach Maßgabe des Absatzes 3a eingewilligt hat. Darüber hinaus ist die Verarbeitung oder Nutzung personenbezogener Daten zulässig, soweit es sich um listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelt, die sich auf die Zugehörigkeit des Betroffenen zu dieser Personengruppe, seine Berufs-, Branchen- oder Geschäftsbezeichnung, seinen Namen, Titel, akademischen Grad, seine Anschrift und sein Geburtsjahr beschränken, und die Verarbeitung oder Nutzung

1. für Zwecke der Werbung für eigene Angebote oder der eigenen Markt- oder Meinungsforschung der verantwortlichen Stelle erforderlich ist, die diese Daten mit Ausnahme der Angabe zur Gruppenzugehörigkeit beim Betroffenen nach § 28 Absatz 1 Satz 1 Nummer 1 erhoben hat,

2. für Zwecke der Werbung oder der Markt- oder Meinungsforschung gegenüber freiberuflich oder gewerblich Tätigen unter deren Geschäftsadresse erforderlich ist oder
3. für Zwecke der Spendenwerbung einer verantwortlichen Stelle erforderlich ist, wenn Spenden an diese gemäß § 10b Absatz 1 und § 34g des Einkommensteuergesetzes steuerbegünstigt sind.

Für Zwecke nach Satz 2 Nummer 1 darf die verantwortliche Stelle zu den dort genannten Daten weitere Daten hinzuspeichern. Die Nutzung personenbezogener Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung ist zudem zulässig, soweit sie zusammen mit Werbung oder Markt- oder Meinungsforschung nach Satz 2 Nummer 1 oder mit der Durchführung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses nach Absatz 1 Satz 1 Nummer 1 erfolgt. Eine Verarbeitung oder Nutzung nach den Sätzen 2 bis 4 ist nur zulässig, soweit schutzwürdige Interessen des Betroffenen nicht entgegenstehen. Nach den Sätzen 1 bis 3 übermittelte Daten dürfen nur für den Zweck verarbeitet oder genutzt werden, für den sie übermittelt worden sind."

e) Nach Absatz 3 werden folgende Absätze 3a und 3b eingefügt:

„(3a) Wird die Einwilligung nach § 4a Absatz 1 Satz 3 in anderer Form als der Schriftform erteilt, hat die verantwortliche Stelle dem Betroffenen den Inhalt der Einwilligung schriftlich zu bestätigen, es sei denn, dass die Einwilligung elektronisch erklärt wird und die verantwortliche Stelle sicherstellt, dass die Einwilligung protokolliert wird und der Betroffene deren Inhalt jederzeit abrufen und die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann. Eine zusammen mit anderen Erklärungen erteilte Einwilligung ist nur wirksam, wenn der Betroffene durch Ankreuzen, durch eine gesonderte Unterschrift oder durch ein anderes, ausschließlich auf die Einwilligung in die Verarbeitung oder Nutzung der Daten für Zwecke des Adresshandels, der Werbung oder der Markt- oder Meinungsforschung bezogenes Tun zweifelsfrei zum Ausdruck bringt, dass er die Einwilligung bewusst erteilt.

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

f) Absatz 4 wird wie folgt geändert:

aa) In Satz 1 wird das Wort „Nutzung“ jeweils durch das Wort „Verarbeitung“ und das Wort „Übermittlung“ jeweils durch das Wort „Nutzung“ ersetzt.

bb) In Satz 2 werden nach dem Wort „Ansprache“ die Wörter „und in den Fällen des Absatz 1 Satz 1 Nummer 1 auch bei Begründung des rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses“ eingefügt.

cc) Satz 3 wird wie folgt geändert:

aaa) Nach dem Wort „Daten“ werden die Wörter „im Rahmen der Zwecke“ eingefügt.

bbb) Das Wort „werden“ wird durch die Wörter „worden sind“ ersetzt.

dd) Folgender Satz wird angefügt:

„In den Fällen des Absatz 1 Satz 1 Nummer 1 darf für den Widerspruch keine strengere Form verlangt werden als für die Begründung des rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses.“

g) In Absatz 9 Satz 4 wird die Angabe „Abs. 3 Nr. 2“ durch die Angabe „Absatz 2 Nummer 2 Buchstabe b“ ersetzt.

6. § 29 wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) In Satz 1 wird nach der Angabe „Markt-“ das Wort „und“ durch das Wort „oder“ ersetzt.

bb) In Satz 2 wird die Angabe „§ 28 Abs. 1 Satz 2“ durch die Angabe „§ 28 Absatz 1 Satz 1 und Absatz 3 bis 3b“ ersetzt.

b) Absatz 2 wird wie folgt geändert:

aa) Satz 1 Nummer 1 wird wie folgt gefasst:

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

bb) In Satz 2 wird die Angabe „§ 28 Abs. 3 Satz 2“ durch die Angabe „§ 28 Absatz 3 bis 3b“ ersetzt.

cc) In Satz 3 wird nach der Angabe „Nummer 1“ die Angabe „Buchstabe a“ gestrichen.

7. In § 33 Absatz 2 Satz 1 Nummer 8 Buchstabe b wird die Angabe „§ 29 Abs. 2 Nr. 1 Buchstabe b“ durch die Angabe „§ 29 Absatz 2 Satz 2“ ersetzt.

8. Nach § 42 wird folgender § 42a eingefügt:

„§ 42a

Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

Stellt eine nichtöffentliche Stelle im Sinne des § 2 Absatz 4 oder eine öffentliche Stelle nach § 27 Absatz 1 Satz 1 Nummer 2 fest, dass bei ihr gespeicherte

1. besondere Arten personenbezogener Daten (§ 3 Absatz 9),
2. personenbezogene Daten, die einem Berufsgeheimnis unterliegen,
3. personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen oder
4. personenbezogene Daten zu Bank- oder Kreditkartenkonten

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

9. § 43 wird wie folgt geändert:
   a) Absatz 1 wird wie folgt geändert:
      aa) Nach Nummer 2 werden folgende Nummern 2a und 2b eingefügt:
      "2a. entgegen § 10 Absatz 4 Satz 3 nicht gewährleistet, dass die Datenübermittlung festgestellt und überprüft werden kann,

2b. entgegen § 11 Absatz 2 Satz 2 einen Auftrag nicht, nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt,"

bb) Nach Nummer 3 wird folgende Nummer 3a eingefügt:

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

b) Absatz 2 wird wie folgt geändert:

aa) In Nummer 5 werden die Angabe", indem er sie an Dritte weitergibt" und am Ende das Wort "oder" gestrichen.

bb) Folgende Nummer 5a wird angefügt:

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

cc) In Nummer 6 wird der Punkt am Ende durch das Wort "oder" ersetzt.

dd) Folgende Nummer 7 wird angefügt:

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

c) Absatz 3 wird wie folgt geändert:

aa) Das Wort „fünfundzwanzigtausend“ wird durch das Wort „fünfzigtausend“ und das Wort „zweihundertfünfzigtausend“ wird durch das Wort „dreihunderttausend“ ersetzt.

bb) Nach Satz 1 werden folgende Sätze eingefügt:

„Die Geldbuße soll den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen. Reichen die in Satz 1 genannten Beträge hierfür nicht aus, so können sie überschritten werden.“

10. Nach § 46 wird folgender § 47 eingefügt:

„§47

Übergangsregelung

Für die Verarbeitung und Nutzung vor dem 1. Juli 2009 erhobener Daten ist § 28 in der bis dahin geltenden Fassung bis zum 1. Juli 2012 weiter anzuwenden.“

Artikel 3

Änderung des Telemediengesetzes[1]

Das Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179) wird wie folgt geändert:

[1] Die Verpflichtungen aus der Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 204 vom 21.7.1998, S. 37), die zuletzt durch die Richtlinie 2006/96/EG vom 20. November 2006 (ABl. L 363 vom 20.12.2006, S. 82) geändert worden ist, sind beachtet worden.

1. In § 11 Absatz 3 wird die Angabe „§ 12 Abs. 3, § 15 Abs. 8 und § 16 Abs. 2 Nr. 2 und 5“ durch die Angabe "§ 15 Absatz 8 und § 16 Absatz 2 Nummer 4" ersetzt.

2. § 12 wird wie folgt geändert:

   a) Absatz 3 wird aufgehoben.

   b) Der bisherige Absatz 4 wird Absatz 3.

3. Nach § 15 wird folgender § 15a eingefügt:

„§ 15a

Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

Stellt der Diensteanbieter fest, dass bei ihm gespeicherte Bestands- oder Nutzungsdaten unrechtmäßig übermittelt worden oder auf sonstige Weise Dritten zur Kenntnis gelangt sind und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen des betroffenen Nutzers, gilt § 42a des Bundesdatenschutzgesetzes entsprechend.“

4. § 16 Absatz 2 wird wie folgt geändert:

   a) Nummer 2 wird aufgehoben.

   b) Die bisherigen Nummern 3 bis 6 werden die Nummern 2 bis 5.

Artikel 4

Änderung des Telekommunikationsgesetzes

Das Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch …, wird wie folgt geändert:

1. Dem § 93 wird folgender Absatz 3 angefügt:

„(3) Stellt der Diensteanbieter fest, dass bei ihm gespeicherte Bestandsdaten oder Verkehrsdaten unrechtmäßig übermittelt worden oder auf sonstige Weise Dritten zur Kenntnis gelangt sind und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen des betroffenen Nutzers, gilt § 42a des Bundesdatenschutzgesetz entsprechend.“

2. In § 95 Absatz 5 werden nach dem Wort „Telekommunikationsdiensten“ die Wörter „ohne die Einwilligung“ eingefügt.

Artikel 5

Bekanntmachungserlaubnis

Das Bundesministerium des Innern kann den Wortlaut des Bundesdatenschutzgesetzes in der vom 1. Juli 2009 an geltenden Fassung im Bundesgesetzblatt bekannt machen.

Artikel 6

Inkrafttreten

(1) Dieses Gesetz tritt vorbehaltlich des Absatzes 2 am Tag nach der Verkündung in Kraft.

(2) Artikel 2, 3 und 4 treten am 1. Juli 2009 in Kraft.

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 Absatz 3 Satz 1 Nummer 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. 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 wirksamen Vorgehen der Aufsichtsbehörden beizutragen. Die vorgeschlagenen Änderungen resultieren in weiten Bereichen aus den Erfahrungen der Länder im Bereich der Aufsichtspraxis. Die Regelungen zur Neugestaltung des § 28 Absatz 3 des Bundesdatenschutzgesetzes finden unabhängig von der Unternehmensgröße Anwendung, jedoch zielen insbesondere die vorgeschlagenen gesetzlichen Erlaubnistatbestände in § 28 Absatz 3 Satz 2 Nummer 2 und Satz 4 auf eine Entlastung spezialisierter kleinerer und mittlerer Unternehmen.

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 informationstechnische 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 informationstechnische 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 informationstechnische 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.

Einem Datenschutzaudit nach Artikel 1 können sich private Unternehmen und diesen gleichgestellte öffentlich-rechtliche Wettbewerbsunternehmen unterziehen. Betroffene Sachmaterie ist daher ganz überwiegend das Recht der Wirtschaft (Artikel 74 Absatz 1 Nummer 11 Grundgesetz). Die Berechtigung des Bundes zur Inanspruchnahme der Gesetzgebungskompetenz ergibt sich aus Artikel 72 Absatz 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 oder informationstechnische 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 informationstechnische Einrichtung in Länder verschärften Kontrollmaßnahmen, käme es unter Umständen dort nicht zum Einsatz. Dies hätte auch Folgen für Verbraucherinnen 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.

Betroffene Sachmaterien des Artikel 2 sind vorwiegend das Bürgerliche Recht (Artikel 74 Absatz 1 Nummer 1 Grundgesetz), das Recht der Wirtschaft (Artikel 74 Absatz 1 Nummer 11 Grundgesetz) und das Arbeitsrecht (Artikel 74 Absatz 1 Nummer 12 Grundgesetz).

Soweit die konkurrierende Gesetzgebungskompetenz des Bundes gemäß Artikel 74 Absatz 1 Nr. 11 Grundgesetz in Anspruch genommen wird, besteht die Erforderlichkeit einer bundesgesetzlichen Regelung gemäß Artikel 72 Absatz 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.

Betroffene Sachmaterie der Artikel 3 und 4 ist das Recht der Wirtschaft (Artikel 74 Absatz 1 Nummer 11 Grundgesetz). Es besteht die Erforderlichkeit einer bundesgesetzlichen Regelung gemäß Artikel 72 Absatz 2 Grundgesetz. Eine bundeseinheitliche Regelung der Informationspflicht bei unbefugter Kenntniserlangung sensibler Daten und des Kopplungsverbots im Telemedien- und Telekommunikationsgesetz ist zur Wahrung der Wirtschaftseinheit im Bundesgebiet im gesamtstaatlichen Interesse erforderlich. Die bestehenden Regelungen des Telemedien- und Telekommunikationsgesetzes können nur durch ein Bundesgesetz geändert werden. Eine ausbleibende Regelung würde zu erheblichen Nachteilen für die Gesamtwirtschaft führen, die im Interesse des Bundes nicht hingenommen werden können. Insbesondere wäre zu befürchten, dass die unterschiedliche Behandlung gleicher Lebenssachverhalte zu erheblichen Wettbewerbsverzerrungen führt. Unternehmen, die dem Telemedien- oder Telekommunikationsgesetz unterliegen, müssten bei einer unbefugten Kenntniserlangung sensibler Daten durch Dritte die Aufsichtsbehörden und die Betroffenen nicht benachrichtigen und unterlägen einem gegenüber der Regelung im Bundesdatenschutzgesetz eingeschränktem Kopplungsverbot. Andere Unternehmen blieben zur Benachrichtigung verpflichtet, obwohl es sich um vergleichbar sensible personenbezogene Daten handelt und dürften in geringerem Umfang Kopplungen vornehmen. Es entstünden für diese dadurch gravierende wettbewerbsverzerrende Änderungen, denen die Unternehmen, die dem Telemedien- oder Telekommunikationsgesetz unterliegen, nicht ausgesetzt wären.

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).

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

Die Stärkung der Unabhängigkeit des Beauftragten für den Datenschutz durch einen erweiterten Kündigungsschutz und die Ermöglichung der Fortbildung fördert die Vorgabe in Artikel 18 Absatz 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.

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 informationstechnischen Einrichtungen sowie der zugelassenen Kontrollstellen.

Für den Vollzugsaufwand beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit können in Abhängigkeit von der Zahl der Kontrollstellen bis zu fünfzehn zusätzliche Stellen sowie jährlich Haushaltsmittel in Höhe von rd. 1,2 Mio. Euro für Personal- und Sachausgaben benötigt werden. Über die Ausbringung und Finanzierung dieser Personal- und Sachausgaben ist im Haushaltsaufstellungsverfahren 2010 zu entscheiden.

V. 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 zu 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 als 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.

VI. Auswirkungen

1. Bürokratiebelastungen für die Wirtschaft

Für die Wirtschaft werden 15 Informationspflichten neu eingeführt und eine Informationspflichten geändert.

Geändert wird die Informationspflicht in § 28 Absatz 3 des Bundesdatenschutzgesetzes. Hier wird partiell die gesetzliche Erlaubnis mit der Möglichkeit des Widerspruchs (§ 28 Absatz 4 Satz 1 des Bundesdatenschutzgesetzes) umgestellt auf eine Einwilligung. Damit entfällt in diesen Fällen die Hinweispflicht bei der Verwendung der Daten zu Gunsten einer Einwilligung von ihrer Weitergabe. Durch diese Änderung entstehen Bürokratiekosten von 9,65 Mio. Euro. Der Betrag errechnet sich bei einer Fallzahl von 30 Mio. Kundenbeziehungen, in denen der Vertragspartner diese Einwilligung anstrebt (Insbesondere Verträge im Versandhandel - 13,5 Mio., Telekommunikation - 13,5 Mio., übrige Gebiete 3 Mio. Fälle), einer Bearbeitungszeit von einer Minute pro Fall und einem Stundensatz von 19,30 Euro. Die Bearbeitungszeit dürfte in der Vielzahl der Fälle bei einer elektronischen Abwicklung deutlich geringer sein. Die angenommene Minute beinhaltet daher auch Aufwand zur Schulung von Mitarbeitern und zur Umstellung von Webseiten.

Durch die übrigen neu eingeführten Informationspflichten entstehen insgesamt Bürokratiekosten von 493.761,00 Euro.

Durch die Änderung des § 28 Absatz 4 Satz 2 des Bundesdatenschutzgesetzes werden nichtöffentliche Stellen verpflichtet, Betroffene über die verantwortliche Stelle und das Widerspruchsrecht in den Fällen des § 28 Absatz 1 Satz 1 Nummer 1 auch bei Begründung des rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses zu unterrichten. § 42a des Bundesdatenschutzgesetzes verpflichtet nichtöffentliche Stellen, die Aufsichtsbehörde und die Betroffenen unverzüglich zu benachrichtigen, wenn bestimmte sensible Daten unrechtmäßig Dritten zur Kenntnis gelangt sind und schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen. 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 Zeitungsseite umfassen, in mindestens zwei bundesweit erscheinenden Tageszeitungen.

Das Datenschutzauditgesetz enthält für die Wirtschaft folgende neue Informationspflichten:

Eine Kontrollstelle hat ihre Zulassung zu beantragen (§ 4 Absatz 1) und kann diese auf einzelne Länder beschränken (§ 4 Absatz 2 Satz 2). Auf Antrag der Kontrollstelle kann ihr eine Ausnahme von der Einbeziehung von einem Datenschutzkonzept oder einer informationstechnischen Einrichtung in ihre Kontrollen gewährt werden (§ 6 Absatz 1 Satz 2). Jährlich hat die Kontrollstelle den zuständigen Behörden ein Verzeichnis der nichtöffentlichen Stellen, die am 31. Dezember des Vorjahres ihrer Kontrolle unterstanden und bis zum 31. März jedes Jahres einen Bericht über ihre Tätigkeit im Vorjahr vorzulegen (§ 6 Absatz 2). Die Kontrollstellen erteilen einander die für eine ordnungsgemäße Durchführung dieses Gesetzes notwendigen Auskünfte (§ 6 Absatz 3 Satz 1). Stellt eine Kontrollstelle Unregelmäßigkeiten oder Verstöße fest, unterrichtet sie unverzüglich die zuständige Behörde (§ 6 Absatz 3 Satz 2). Soweit eine Kontrollstelle im Rahmen der von ihr durchgeführten Kontrollen Tatsachen feststellt, die einen hinreichenden Verdacht auf Verstöße der in Satz 2 genannten Art begründen, der eine nicht von der Kontrollstelle kontrollierte nichtöffentliche Stelle betrifft, teilt die Kontrollstelle die Tatsachen unverzüglich der Kontrollstelle mit, deren Kontrolle die betroffene nichtöffentliche Stelle untersteht (§ 6 Absatz 3 Satz 3). Die Kontrollstelle unterrichtet die von ihr kontrollierten nichtöffentlichen 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 (§ 6 Absatz 4 Satz 1). Die nichtöffentlichen Stellen sowie die Kontrollstellen haben den zuständigen Behörden auf Verlangen Auskünfte zu erteilen (§ 8 Absatz 1). Auf ihr Aussageverweigerungsrecht sind sie hinzuweisen (§ 8 Absatz 4 Satz 2). Vor der erstmaligen Verwendung des Datenschutzauditsiegels ist das Datenschutzkonzept oder die informationstechnische Einrichtung dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit anzuzeigen (§ 9 Absatz 1 Satz 1).

Die Summe der zu erwartenden Belastungen für die Wirtschaft beträgt insgesamt 10,14 Mio. Euro.

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

2. Bürokratiebelastungen für die Bürgerinnen und Bürger

Für die Bürgerinnen und Bürger wird keine Informationspflicht neu eingeführt geändert oder abgeschafft.

3. Bürokratiebelastungen für die Verwaltung

Für die Verwaltung werden zwölf Informationspflichten neu eingeführt und keine Informationspflichten geändert oder abgeschafft.

Diese Informationspflichten sind im Einzelnen:

§ 7 Absatz 1 Satz 2 Datenschutzauditgesetz	Auskunftserteilung der zuständigen Behörden untereinander.
§ 7 Absatz 1 Satz 3 Nummer 1 Datenschutzauditgesetz	Mitteilungspflicht der zuständigen Behörde zur Anregung der Entziehung der Zulassung oder Änderung von Auflagen an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit
§ 7 Absatz 1 Satz 3 Nummer 2 Datenschutzauditgesetz	Mitteilungspflicht an die zuständige Behörde des Landes
§ 7 Absatz 1 Satz 4 Datenschutzauditgesetz	Mitteilungspflicht der zuständigen Behörde zur Anregung eines Verfahrens der Entziehung der Zulassung oder Änderung von Auflagen an den
§ 8 Absatz 4 Satz 2 Datenschutzauditgesetz	Hinweispflicht gegenüber dem Auskunftspflichtigen
§ 9 Absatz 1 Satz 2 Datenschutzauditgesetz	Führung eines Verzeichnisses für Datenschutzkonzepte durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit
§ 9 Absatz 1 Satz 2 Datenschutzauditgesetz	Veröffentlichungspflicht im Internet und im elektronischen Bundesanzeiger
§ 9 Absatz 2 Satz 1 Datenschutzauditgesetz	Führung eines Verzeichnisses der zugelassenen Kontrollstellen
§ 9 Absatz 2 Satz 1 Datenschutzauditgesetz	Veröffentlichungspflicht im Internet und im elektronischen Bundesanzeiger
§ 11 Absatz 1 Satz 3 Datenschutzauditgesetz	Veröffentlichungspflicht der maßgeblichen Richtlinien im Internet und im elektronischen Bundesanzeiger
§ 15 Absatz 2 Satz 3 Datenschutzauditgesetz	Berichtspflicht an die Aufsichtsbehörde
§ 15 Absatz 3 Satz 1 Datenschutzauditgesetz	Pflicht der Genehmigung durch die Aufsichtsbehörde

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.

VII. Auswirkungen von gleichstellungspolitischer Bedeutung

Auswirkungen von gleichstellungspolitischer Bedeutung sind nicht zu erwarten.

B. Besonderer Teil

Zu Artikel 1

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 Anbieter von Datenverarbeitungsanlagen und -programmen für die von ihnen angebotenen Datenverarbeitungsanlagen und –programme und verantwortliche Stellen nach § 3 Absatz 7 des Bundesdatenschutzgesetzes hinsichtlich ihrer Datenschutzkonzepte. Anbieter stellen anderen, auch unentgeltlich, eine Datenverarbeitungsanlage oder Datenverarbeitungsprogramm oder beides zur Verfügung, sei es als Hersteller oder in anderer Form am Vermarktungsprozess Beteiligter. Datenverarbeitungsanlage (Hardware) und Datenverarbeitungsprogramm (Software) bilden zusammen ein Datenverarbeitungssystem. Sie sind gesondert aufgeführt, um zu verdeutlichen, dass auch nur eine Datenverarbeitungsanlage oder nur ein Datenverarbeitungsprogramm Auditgegenstand sein kann. Eine Datenverarbeitungsanlage ist ein Gerät oder eine Baueinheit zur Verarbeitung von Daten. Der Begriff findet sich bereits verschiedentlich im Bundesdatenschutzgesetz, z. B. in § 1 Absatz 2 Nummer 3, § Absatz 2 Satz 1, § 11 Absatz 5, § 14 Absatz 4, § 18 Absatz 2 Satz 1, § 27 Absatz 1 Satz 1, § 31 und Nummer 1 der Anlage zu § 9 Satz 1 und anderen Bundesgesetzen, z. B. in § 9 Absatz 1 Satz 2 des Antiterrordateiengesetzes, § 9Absatz 2 Satz 21 des Ausländerzentralregistergesetzes oder § 11 Absatz 6 Satz 2 des Bundeskriminalamtsgesetzes. Datenverarbeitungsprogramme steuern die automatisierte Verarbeitung personenbezogener Daten. Auch dieser Begriff findet sich neben § 9a bereits verschiedentlich im Bundesdatenschutzgesetz, z. B. in § 4g Absatz 1 Satz 4 Nummer 1, § 24 Absatz 4 Satz 2 Nummer 1 und § 38 Absatz 4 Satz 2 sowie in anderen Bundesgesetzen, z. B. in § 4 Absatz 2 Nummer 3 des Außenwirtschaftsgesetzes (der das Synonym „Software“ verwendet).

Einem Datenschutzaudit können sich Anbieter von Datenverarbeitungsanlagen und -programmen und verantwortliche Stellen unterziehen, sofern sie „nichtöffentliche Stelle im Sinne des § 2 Absatz 4 des Bundesdatenschutzgesetzes sind“. Die Einschränkung bezieht sich sowohl auf die Anbieter von Datenverarbeitungsanlagen und -programmen als auch auf 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 informationstechnische 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 Daten-

schutz-audit einzuführen, wie es z. B. in der Freien Hansestadt Bremen oder Schleswig-Holstein geschehen ist.

Gegenstand der Prüfung und Bewertung können Datenschutzkonzepte sowie informationstechnische Einrichtungen sein. Ein Datenschutzkonzept ist eine geordnete Darstellung, auf welche Weise die Anforderungen des Datenschutzes und der Datensicherheit erfüllt werden. Bezugspunkt für ein Datenschutzkonzept ist entweder eine verantwortliche Stelle oder ein abgrenzbarer Teilbereich hiervon (z. B. die IT-Abteilung, die Personalabteilung, das Archiv). Bezugspunkt kann auch ein Verfahren automatisierter Verarbeitung oder ein abgrenzbarer Teilbereich hiervon sein. Bestandteil des Datenschutzkonzepts ist insbesondere der Inhalt der Meldepflicht nach § 4e Satz 1 des Bundesdatenschutzgesetzes, gegebenenfalls die Nennung des Beauftragten für den Datenschutz sowie Angaben zu den verwendeten informationstechnischen Einrichtungen. Bestandteil der Darstellung sind die getroffenen bzw. geplanten technischen und organisatorischen Maßnahmen nach § 9 des Bundesdatenschutzgesetzes, die nach der Anlage zu § 9 Satz 1 des Bundesdatenschutzgesetzes auch die Ausgestaltung der innerbetrieblichen Organisation umfassen. Bestandteil ist auch ein Sicherheitskonzept, das eine Analyse der bestehenden Risiken enthält, eine Schutzzweckbeschreibung, die Beschreibung der Maßnahmen zur technischen und organisatorischen Sicherheit und die verbleibenden Risiken. Eine informationstechnische Einrichtung ist eine Hardware oder Software, mit der eine verantwortliche Stelle die personenbezogenen Daten automatisiert verarbeitet.

Die Unternehmen können 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 Datenschutzkonzept oder eine informationstechnische Einrichtung mit einem Datenschutzauditsiegel gekennzeichnet werden darf.

Nach Nummer 1 sind die Vorschriften zum Schutz personenbezogener Daten bei der Datenverarbeitung einzuhalten, für die das Datenschutzkonzept oder die informationstechnische Einrichtung vorgesehen ist. Grundlage für die Verwendung ist also, dass die Datenverarbeitung, die Gegenstand des Datenschutzkonzepts oder der informationstechnischen Einrichtung ist, vor Ort gesetzeskonform und im Einklang mit den Vorgaben der europäischen Datenschutzrichtlinie 95/46/EG 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 informationstechnische Einrichtung ein Datenschutzauditsiegel begehrt. Der Begriff der „Datenverarbeitung“ meint nicht den Begriff der „Verarbeitung nach § 3 Absatz 4 des Bundesdatenschutzgesetzes, da auch die Erhebung oder Nutzung personenbezogener Daten Gegenstand des Auditgegenstandes sein kann.

Nach Nummer 2 muss der Auditgegenstand die vom Datenschutzauditausschuss beschlossenen und veröffentlichten Richtlinien zur Verbesserung des Datenschutzes und

der Datensicherheit nach § 11 Absatz 1 erfüllen. Ein Datenschutzauditsiegel, das bereits für die Einhaltung der Vorschriften über den Schutz personenbezogener Daten (Gesetzeskonformität) erlangt werden kann, 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 Absatz 1 Satz 1 des Bundesdatenschutzgesetzes und die Aufsichtsbehörden nach § 38 des Bundesdatenschutzgesetzes kontrolliert. Ein auf die Gesetzeskonformität beschränktes Datenschutzauditsiegel liefe damit Gefahr, die bestehenden Kontrollen zu entwerten oder zumindest eine Verfahrensdoppelung herbeizuführen. Es bestünde 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 informationstechnische 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 informationstechnische 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 Kennzeichnung mit einem Datenschutzauditsiegel, dass Anbieter im Inland die Vorschriften des Bundesdatenschutzgesetzes über die organisatorische Stellung des Beauftragten für den Datenschutz einhalten. Hierzu gehören insbesondere § 4f Absatz 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 Absatz 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. Die Regelung führt nicht zu einer abweichenden Verpflichtung zur Bestellung bei Durchführung eines Datenschutzaudits.

Nach Nummer 4 ist Voraussetzung für die Kennzeichnung mit einem Datenschutzauditsiegel, dass die Nummern 1 bis 3 nach § 3 kontrolliert 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 verwiesen.

Soweit öffentliche Stellen als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, finden auf sie nach § 27 Absatz 1 Satz 1 Nummer 2 des Bundesdatenschutzgesetzes dieselben Vorschriften Anwendung wie auf nichtöffentliche Stellen. Sie sind diesen gleichgestellt. Im Wettbewerb mit nichtöffentlichen 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 nichtöffentlichen Konkurrenten zu verschaffen.

Zu § 2 (Zuständigkeit)

Absatz 1:

Die Regelung der Behördenzuständigkeit bleibt hier grundsätzlich - soweit nichts anderes bestimmt wird - den Ländern überlassen. Das Verfahren der Kontrolle soll 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 Absatz 4 des Telekommunikationsgesetzes und § 42 Absatz 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 oder verwendet 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 Vergabe einer Kennnummer an die zugelassenen Kontrollstellen 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 Absatz 1 und § 4 Absatz 4 verwiesen.

Zu § 3 (Kontrollen)

Nachdem in § 2 Absatz 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 nach § 7 Absatz 2, 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 Absatz 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 Begleitung der 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 Absatz 3 Nummer 3 näher auszuführenden Mindestkontrollanforderungen und im Rahmen des Kontrollverfahrens vorgesehenen Vorkehrungen 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 Verstößen gegen dieses Gesetz, die auf Grund dieses Gesetzes erlassenen Rechtsverordnungen und die für den Auditgegenstand geltenden Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit nach § 11 Absatz 1 bestimmen.

Satz 4 und 5 legen neben der risikobasierten Häufigkeit der Kontrollen die Mindesthäufigkeit der Kontrollen fest. Jedes in das Kontrollsystem einbezogene Unternehmen soll nach der Anzeige der Verwendung des Datenschutzauditsiegels an den Beauftragten für den Datenschutz und die Informationsfreiheit nach § 9 Absatz 1 Satz 1 sobald es der ordnungsgemäße Geschäftsbetrieb der Kontrollstelle erlaubt, einer ersten Kontrolle und vor Ablauf von zwölf Monaten nach dem Abschluss dieser Erstkontrolle einer weiteren, zweiten Kontrolle unterzogen werden. Im Anschluss an die zweite Kontrolle ist es aufgrund der dann vorhandenen Kenntnisse über das Datenschutzkonzept oder die informationstechnische Einrichtung gerechtfertigt, die Mindesthäufigkeit der Kontrollen auf achtzehn Monate auszudehnen, zumal die Möglichkeit, zusätzliche Kontrollen vorzunehmen, z. B. wenn Verstöße aufgetreten sind, unberührt bleibt. Die Mindesthäufigkeit der Kontrollen soll nach drei Jahre mit Blick auf Auswirkungen und Effektivität evaluiert werden.

Die auf Grundlage des Bundesdatenschutzgesetzes und der Datenschutzgesetze der Länder durchgeführten Kontrollen bleiben 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 Absatz 1 Rechnung. Nach Satz 1 Nummer 1 sind Kontrollstellen zuzulassen,

wenn ihr Leitungspersonal und die für Kontrollen verantwortlichen Beschäftigten über die erforderliche persönliche Zuverlässigkeit, Unabhängigkeit und fachliche Eignung verfügen, die näher in § 5 aufgeführt ist. Nach Satz 1 Nummer 2 muss die Kontrollstelle in organisatorischer Hinsicht akkreditiert sein, wie in anderen Bereichen bereits praktiziert. Als angemessene und anerkannte Akkreditierungsgrundlage kommt für Datenschutzkonzepte z. B. die ISO/IEC 17021:2006 (Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren) oder für den Bereich der informationstechnischen Einrichtungen z. B. die DIN EN 45011 (Allgemeine Anforderungen an Stellen, die Produktzertifizierungssysteme betreiben) oder die ISO/IEC 17025:2005 (Allgemeine Anforderungen an die Kompetenz von Prüf- und Kalibrierlaboratorien) in Frage. Näheres regelt die nach § 16 Absatz 3 Nummer 2 zu erlassene Rechtsverordnung. Nach Satz 1 Nummer 3 und 4 wird neben der Entrichtung der für die Zulassung erhobenen Gebühren das Unterhalten des Sitzes oder einer Niederlassung im Bundesgebiet 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.

Nach Satz 2 wird der Kontrollstelle mit der Zulassung eine Kennnummer zugeteilt, über die ein mit einem Datenschutzauditsiegel gekennzeichnetes Datenschutzkonzept oder eine informationstechnische Einrichtung auf die Kontrolle einer bestimmten Kontrollstelle zurückgeführt werden kann.

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 § 6 Absatz 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 die Funktionsfähigkeit des Kontrollsystems“ dies erfordert, soll auch 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 nach Absatz 1 Satz 1 Nummer 1, 2 oder 4 für die Zulassung nicht mehr erfüllt und wenn sie Verpflichtungen nach diesem Gesetz oder einer aufgrund dieses Ge-

setzes erlassenen Rechtsverordnung in schwerwiegender Weise nicht nachkommt. Die Hervorhebung der Verpflichtungen nach § 6 oder § 8 Absatz 3 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 (Anforderungen an das Personal der Kontrollstelle)

Die Vorschrift regelt im Einzelnen die Anforderungen an Kontrollstellen zum Nachweis der nach § 4 Absatz 1 Nummer 1 geforderten erforderlichen 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 Absatz 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 Erstreckung der Anforderungen auf weitere Beschäftigte, die keine Verantwortung für die Kontrollen tragen, ist nicht erforderlich und angemessen.

Zu § 6 (Pflichten der Kontrollstelle)

Absatz 1:

Absatz 1 Satz 1 gibt dem Unternehmen einen Anspruch darauf, in das Kontrollsystem einbezogen zu werden, wenn es die Bestimmungen des Gesetzes einhält und seinen Beitrag zu den Kosten des Kontrollverfahrens entrichtet. Der tatsächlichen Zulassung der Kontrollstelle in dem betroffenen Land soll die Regelung nach § 4 Absatz 3 Satz 1 (soweit die Funktionsfähigkeit des Kontrollsystems dies 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 Ausnahme von der Verpflichtung 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 Nummer 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 bis zum 31. Januar ein Verzeichnis der Unternehmen, die am 31. Dezember des Vorjahres ihrer Kontrolle unterstanden. Die Kontrollstelle legt ferner bis zum 31. März jedes Jahres einen zusammenfassenden Bericht über die im Vorjahr ausgeführte Kontrolltätigkeit vor. Dabei sind insbesondere alle festgestellten Abweichungen und Verstöße sowie die getroffenen Maßnahmen zu dokumentieren.

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.

Nach Satz 2 hat die Kontrollstelle über bei ihrer Tätigkeit festgestellte Verstöße gegen die in § 1 Satz 2 Nummer 1 bis 3 genannten Vorschriften unverzüglich die zuständige Behörde zu unterrichten. Korrespondierend mit dieser ausnahmslosen Unterrichtung an die zuständige Behörde ist es deren Ermessensentscheidung nach § 7 Absatz 2, inwieweit weiterhin eine Kennzeichnung erfolgen darf. Die Entscheidung, wie sich ein Verstoß auswirkt, soll aufgrund der Tragweite die zuständige Behörde treffen und nicht die private Kontrollstelle. Dies führt auch zu größerer Einheitlichkeit und Systemgerechtigkeit insgesamt, da es nur 16 Landesbehörden und den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit als zuständige Behörden gibt, jedoch eine im einzelnen noch nicht abzuschätzende Vielzahl von Kontrollstellen. Ein eingeschränkter Informationsfluss zwischen zuständiger Behörde und Kontrollstelle berührt auch das System der Aufgabenübertragung. Eine zuständige Behörde wird im Zweifel keine Aufgaben an eine Kontrollstelle übertragen, wenn sie nicht vollständig informiert wird. Die Unterrichtung über Verstöße an die zuständige Behörde dient ferner dem Aufbau von Erfahrungswissen über Probleme am Markt und damit der Qualitätssicherung der Verfahren.

Mit Satz 3 sollen die Melde- und Informationspflichten der Kontrollstellen für den Fall präzisiert werden, dass sich ein begründeter Verdacht auf 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 festgestellten Verstöße ihren Ursprung bei einem anderen Unternehmen haben. 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 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 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 § 7 (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 Absatz 2 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 Absatz 4 resultiert regelmäßig aus dem Überwachungsverfahren, das nach Satz 1 den zuständigen Behörden 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 zuständige Behörde für eine Kontrollstelle, die aufgrund 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 dem 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 Absatz 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 Absatz 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. Bei der Ermessensentscheidung sollen unter anderem die Bedeutung der Vorschrift, gegen die verstoßen wurde, sowie die Art und die besonderen Umstände des Verstoßes einbezogen werden, z. B. auch der Umstand, dass der Verstoß bereits beseitigt worden ist. Bei schwerwiegenden Verstößen oder Verstößen mit Langzeitwirkung kann die Kennzeichnung für einen von der zuständigen Behörde bestimmten Zeitraum untersagt werden, z. B. weil es zunächst erforderlich ist, ein Produkt oder Verfahren technisch nachzubessern oder organisatorische Maßnahmen umzusetzen.

Zu § 8 (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 Absatz 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 zur Gewährleistung eines hohen Qualitätsniveaus des Kontrollsystems 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 § 9 (Datenschutzauditsiegel, Verzeichnisse)

Absatz 1:

Absatz 1 verfolgt das Ziel, das Internet und den elektronischen Bundesanzeiger zur Feststellung der Echtheit von mit einem Datenschutzauditsiegel gekennzeichneten Datenschutzkonzepten oder informationstechnischen 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 informationstechnische Einrichtung mit dem Datenschutzauditsiegel kennzeichnen 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 Absatz 3 Nummer 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 und informationstechnischen 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 für andere Wirtschaftsbeteiligte eine Informationsmöglichkeit geschaffen, um sichere Auskünfte über die Echtheit der betroffenen Datenschutzkonzepte sowie informationstechnischen 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 Betroffenen. 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 informationstechnische Einrichtung ein Datenschutzauditsiegel zu verwenden.

Absatz 2:

Absatz 2 sieht in gleicher Weise wie in Absatz 1 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 aufge-

führt. Damit wird es u. a. den Unternehmen ermöglicht, für sie in Frage kommende Kontrollstellen ausfindig zu machen.

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 Absatz 1 Satz 2 und Absatz 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 § 9 Absatz 1 und 2. Dazu zählen die Entgegennahme der Anzeige der Verwendung des Datenschutzauditsiegels sowie die Aufnahme der angezeigten Datenschutzkonzepte und informationstechnischen Einrichtungen und weiterer Daten in einem Verzeichnis im Internet sowie im elektronischen Bundesanzeiger.

Für die Bemessung der Gebühren ordnet Satz 1 das Kostendeckungsprinzip an. Damit gilt nach § 3 Absatz 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 § 7 Absatz 1 Satz 1 und Absatz 2 den Ländern obliegt.

Zu § 11 (Datenschutzauditausschuss)

Absatz 1:

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

Satz 2 bestimmt die Aufgabe des Datenschutzauditausschusses, Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit zu erlassen. Einige Inhalte, durch die Richtlinien über den bestehenden Stand der Gesetze hinaus Verbesserungen des Datenschutzes und der Datensicherheit erreichen können, sind nicht abschließend aufgeführt. Die Transparenz der Datenerhebung, -verarbeitung und -nutzung wird dabei auch durch die Auskunftsrechte der Betroffenen gewährleistet. Die Aufzählung berührt nicht die Entscheidung des Ausschusses, welche Richtlinien er inhaltlich vorrangig angeht und mit welchen Inhalten 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 unterrichtet der Datenschutzauditausschuss jährlich die Öffentlichkeit in einem 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 zu erlassen, 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 hierauf 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 diese Aspekte einzubringen,

- Vertreter von Aufsichtsbehörden der Länder für den Datenschutz im nichtöffentlichen Bereich, da sie die ordnungsgemäßen Kontrollen der Kontrollstellen überwachen und um aufsichtsbehördliche 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 um 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 Absatz 3 Nummer 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, Unparteilichkeit 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 Absatz 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 nichtöffentlichen 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.

Absatz 4:

Zu Sitzungen des Datenschutzauditausschusses ist ein Vertreter der Bundesnetzagentur mit beratender Stimme hinzuzuziehen, soweit Gegenstand der Sitzung eine Richtlinie ist, die nichtöffentliche Stellen betrifft, die nach § 115 Absatz 4 Satz 1 des Telekommunikationsgesetzes oder § 42 Absatz 3 des Postgesetzes der Kontrolle des Bundesbeauftragten unterliegen.

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, z. B. der Bundesnetzagentur im Bereich der Post und Telekommunikation, die Niederschrift, die Einsetzung von thematischen 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 Mitglieder.

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 Absatz 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 Absatz 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 die Bundesregierung, deren Rechtsaufsicht der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit nach § 22 Absatz 4 Satz 3 des Bundesdatenschutzgesetzes unterliegt, nach Anhörung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit ohne Zustimmung des Bundesrates.

Absatz 3:

Die Vorschrift sieht in Absatz 3 Nummer 1 die erforderliche Ermächtigung des Bundesministeriums des Innern vor, um im Wege einer Rechtsverordnung mit Zustimmung des Bundesrates Einzelheiten der Verwendung des Datenschutzauditsiegels zu regeln, um

eine einheitliche Kennzeichnung und eindeutige Erkennbarkeit der Kennzeichnung zu gewährleisten.

Nummer 2 eröffnet die Möglichkeit, erforderlichenfalls die Voraussetzungen, 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.

Die Nummern 4 und 5 sehen vor, die Gestaltung des Datenschutzauditsiegels und die Anzeige seiner Verwendung nach § 9 Absatz 1 Satz 1 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, z. B. im Hinblick auf § 4 Absatz 1 Satz 1 Nummer 2, näher ausführen. Die Rechtsverordnung nach Nummer 3 soll Einzelheiten zu den Mindestanforderungen an das Kontrollverfahren 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 (Bußgeldvorschriften)

Die Vorschrift enthält die erforderlichen Bußgeldtatbestände, insbesondere bei vorsätzlich oder fahrlässig unbefugter Kennzeichnung mit dem Datenschutzauditsiegel entgegen einer Anordnung der zuständigen Behörde oder bei unzureichender Anzeige der Verwendung gegenüber dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit durch Unternehmen.

Für Kontrollstellen soll es einen Bußgeldtatbestand darstellen, ein Verzeichnis der kontrollierten Stellen oder einen Kontrollbericht nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig vorzulegen sowie nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig über festgestellte 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 Maßnahmen nicht zu dulden oder eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig zu erteilen.

Der Strafrahmen entspricht demjenigen nach § 43 Absatz 3 in Verbindung mit Absatz 1 bzw. 2 des Bundesdatenschutzgesetzes.

Zu § 18 (Strafvorschrift)

Die Vorschrift stellt die vorsätzliche unbefugte Kennzeichnung mit einem Datenschutzauditsiegel entgegen der Anordnung einer zuständigen Behörde nach § 7 Absatz 2 in Bereicherungs- oder Schädigungsabsicht unter Strafe. Der Strafrahmen entspricht demjenigen nach § 44 Absatz 1 des Bundesdatenschutzgesetzes.

Zu § 19 (Einziehung)

Die Vorschrift enthält die übliche nebenstrafrechtliche Regelung.

Zu § 20 (Übergangsvorschrift)

Die Möglichkeit, ein Datenschutzaudit nach dem Datenschutzauditgesetz durchzuführen, ist abhängig von verschiedenen vorbereitenden Maßnahmen, insbesondere der Konstituierung des Datenschutzauditausschusses und der Erarbeitung und dem Beschluss von Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit als Grundlage für die Kennzeichnung mit dem Datenschutzauditsiegel. § 1 ist daher erst ab dem 1. Juli 2010 anzuwenden.

Zu Artikel 2

Zu Nummer 1 (Inhaltsübersicht):

Die Inhaltsübersicht ist an die nachfolgend begründeten Gesetzesänderungen anzupassen.

Zu Nummer 2 (§ 4f Absatz 3 Satz 5 bis 7)

Durch die Änderung soll die Position des Beauftragten für den Datenschutz gestärkt werden. Satz 5 erweitert den Kündigungsschutz des Beauftragten für den Datenschutz. Satz 6 erstreckt diesen Kündigungsschutz auf die Zeit nach Beendigung der Funktion des Beauftragten für den Datenschutz. Satz 7 unterstützt die Fortbildung und damit die fachliche Eignung des Beauftragten für den Datenschutz.

Satz 5 passt den Kündigungsschutz der Beauftragten für den Datenschutz, die Arbeitnehmer der zur Bestellung verpflichteten Stelle sind, an den Kündigungsschutz vergleichbarer Funktionsträger an, wie z.B. des Gewässerschutzbeauftragten (§ 21f Absatz 2 Satz 1, 2 des Wasserhaushaltsgesetzes), des Immissionsschutzbeauftragten (§ 58 Absatz 2 Satz 1, 2 des Bundesimmissionsschutzgesetzes), des Störfallbeauftragten (§ 58d i. V. m. § 58 Absatz 2 Satz 1, 2 des Bundesimmissionsschutzgesetzes), des Abfallbeauftragten (§ 55 Absatz 3 des Kreislaufwirtschafts-/Abfallgesetzes i. V. m. § 58 Absatz 2 Satz 1, 2 des Bundesimmissionsschutzgesetzes) oder der Betriebsratsmitglieder (§ 15 Absatz 1 Satz 1, 2 des Kündigungsschutzgesetzes). Die Aufgabenstellung des Beauftragten für den Datenschutz mit diesen privilegiert geschützten Funktionsträgern ist nach Art und Umfang vergleichbar. Allen diesen Beauftragten ist gemeinsam, dass die Einhaltung gesetzlicher Vorschriften überwacht und hierfür Kontrollen durchgeführt werden. Darüber hinaus wirken sie für ihren Aufgabenkreis auf eine Verbesserung der bestehenden Situation hin,

informieren die Beschäftigten und beraten die verantwortliche Stelle. Derzeit ist dem Beauftragten für den Datenschutz in § 4f Absatz 3 Satz 3 und 4 ein Benachteiligungsverbot und eine erschwerte Abberufung eingeräumt. Diese hat sich in der Praxis als nicht ausreichend erwiesen, vor allem dann – was der Regelfall ist – wenn die Aufgabe des Beauftragten für den Datenschutz nur als Teilaufgabe wahrgenommen wird. Ein Widerruf der Bestellung des Beauftragten für den Datenschutz kann gemäß § 4f Absatz 3 Satz 4 in entsprechender Anwendung des § 626 des Bürgerlichen Gesetzbuchs (und bei nichtöffentlichen Stellen auf Verlangen der Aufsichtsbehörde) erfolgen. Verschiedene Arbeitsgerichte, haben unter teilweise ausdrücklicher Bezugnahme auf die unterschiedliche gesetzliche Regelung des Kündigungsschutzes bei Beauftragten für den Datenschutz gegenüber anderen Funktionsträgern entschieden, dass eine ordentliche Kündigung aus anderen als amtsbezogenen Gründen durch die bestehenden Regelungen in § 4f Absatz 3 Satz 3 und 4 nicht ausgeschlossen ist. Sie haben weiter gefolgert, dass mit dem beendeten Arbeitsverhältnis zugleich die Bestellung als Beauftragter für den Datenschutz beendet ist und es einer ausdrücklichen Abberufung nicht mehr bedarf (z.B. Landesarbeitsgericht Niedersachsen, Urteil vom 16. Juni 2003, - 8 Sa 1968/02; Landesarbeitsgericht Berlin, Urteil vom 27. Oktober 1997, - 17 Sa 87/97). Das Bundesarbeitsgericht hat bislang lediglich entschieden, dass eine Teilkündigung der arbeitsvertraglichen Abrede zur Übernahme des Amtes eines Beauftragten für den Datenschutzbeauftragten zulässig ist und Prüfungsmaßstab gleichlaufend mit der Abberufung nach § 4f Absatz 3 Satz 4 der § 626 des Bürgerlichen Gesetzbuchs sein muss (Urteil vom 13. März 2007, - 9 AZR 612/05). Das Bundesarbeitsgericht hat sich nicht dazu geäußert, ob auch eine ordentliche Kündigung des Arbeitsverhältnisses möglich wäre und inwieweit dies zur Beendigung des Amtes des Datenschutzbeauftragten führen würde. Diese Frage wird durch Satz 5 geklärt. Durch die Anknüpfung an die zur Bestellung verpflichteten Stellen nach 4f Absatz 1 Satz 1 kommt zum Ausdruck, dass ein Kündigungsschutz nicht besteht, wenn die Stelle sich freiwillig dazu entscheidet, einen Beauftragten für den Datenschutz zu bestellen. Eine Ausdehnung des Kündigungsschutzes auch auf nicht zur Bestellung verpflichtete Stellen würde diese im Ergebnis davon Abhalten, freiwillig einen Beauftragten für den Datenschutz zu bestellen und führt zu einem ungewollten Ergebnis. Satz 5 stellt klar, dass der in Satz 5 und 6 vorgesehene Kündigungsschutz nicht zusätzlich und separat vom Kündigungsschutzgesetz gewährt wird. Finden die Regelungen zum allgemeinen Kündigungsschutz in einem Betrieb keine Anwendung, etwa weil zu wenig Arbeitnehmer beschäftigt werden, besteht jedoch nach § 4f Absatz 1 Satz 6 unabhängig von der Anzahl der mit der automatisierten Verarbeitung beschäftigten Personen eine Verpflichtung zur Bestellung eines Beauftragten für den Datenschutz, so besteht auch kein Kündigungsschutz nach Satz 5 und 6.

Satz 6 beinhaltet einen nachwirkenden Kündigungsschutz, indem er diesen, ebenfalls in Anlehnung an die o.g. Vorschriften bei vergleichbaren Funktionsträgern, auf ein Jahr nach Beendigung des Amtes des Beauftragten für den Datenschutz erstreckt.

Satz 7 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 Absatz 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 des 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 Absatz 6 Satz 1 des Betriebsverfassungsgesetzes, § 46 Absatz 6 des Bundespersonalvertretungsgesetzes).

Zu Nummer 3 (§ 9a)

Der bisherige § 9a sieht die Möglichkeit eines Datenschutzaudits vor und kündigt in Satz 2 ein Gesetz hierzu an. Dieses ist in Art. 1 vorgesehen. § 9a wird dadurch obsolet.

Zu Nummer 4 (§ 12 Absatz 4)

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

Zu Nummer 5 (§ 28)

Die vorgeschlagene Regelung beinhaltet die Streichung des bisher in § 28 Absatz 3 Satz 1 Nummer 3 geregelten sog. „Listenprivilegs“ und die Einführung eines begrenzten Kopplungsverbots für marktbeherrschende Unternehmen im neuen Absatz 3b. Die weiteren Änderungen sind redaktionelle Änderungen und Folgeänderungen.

Die Überschrift des § 28 wird an die Überschrift des § 29 angepasst.

In Absatz 1 Satz 1 Nummer 1 werden aufgrund der Schuldrechtsnovelle des Jahres 2002 die Begriffe „Vertragsverhältnis“ und „vertragsähnliches Vertrauensverhältnis“ in Anpassung an die durch die Schuldrechtsnovelle des Jahres 2002 eingeführte Terminologie durch die Begriffe „rechtsgeschäftliches Schuldverhältnis“ und „rechtsgeschäftsähnliches Schuldverhältnis“ (vgl. z. B. § 311 des Bürgerlichen Gesetzbuchs) ersetzt.

Die bisherigen Absätze 2 und 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 Absatz 3 Satz 1 durch das Wort „auch“ zum Ausdruck. Der bisherige Absatz 2 ist nunmehr Absatz 2 Nummer 1. Die bisherigen Erlaubnistatbestände in Absatz 3 Satz 1 Nummer 1 und 2 sind sprachlich zusammengefasst worden und nunmehr Absatz 2 Nummer 2 Buchstabe a und b. Die bisherige Absatz 3 Satz 1 Nummer 4 ist nunmehr Absatz 2 Nummer 3.

Der bisherige Absatz 3 Satz 1 Nummer 3, das sog. „Listenprivileg“, wurde gestrichen. Der bisherige § 28 Absatz 3 Satz 2 wurde infolge der Neuregelung in Absatz 3 entbehrlich. Der neue Absatz 3 Satz 1 hält zunächst als Grundsatz fest, dass die Verwendung personenbezogener Daten für Zwecke des Adresshandels, der Werbung oder der Markt- oder Meinungsforschung zulässig ist, wenn der Betroffene entsprechend den Vorgaben des Absatzes 3a eingewilligt hat. Dies ergibt sich allgemein bereits aus § 4 Absatz 1 2. Alternative, jedoch sieht Absatz 3a insoweit eine Konkretisierung der wegen besonderer Umstände angemessenen Form nach § 4a Absatz 1 Satz 3 vor. Die verantwortliche Stelle muss insoweit 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 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 wird nicht vor-

gegeben und bleibt den individuellen Bedürfnissen der Wirtschaft entsprechend ihr überlassen, wird aber mit gewissen Kosten verbunden sein.

Die Verwendung ist darüber hinaus nach dem Absatz 3 Satz 2 bis 5 als gesetzliche Erlaubnis im Sinne des § 4 Absatz 1 1. Alternative zulässig. Diese gesetzliche Erlaubnis berührt selbstverständlich nicht die gesetzlichen Anforderungen des § 11, soweit eine Auftragsdatenverarbeitung erfolgt. Absatz 3 Satz 2 beschränkt die gesetzliche Erlaubnis für die Nummern 1 bis 3 generell auf die Verwendung der bisher in § 28 Absatz 3 Satz 1 Nummer 3 aufgeführten sog. „Listendaten“.

Nach dem Absatz 3 Satz 2 Nummer 1 muss es sich um Werbung für eigene Angebote oder eigene Markt- oder Meinungsforschung handeln. Die Verwendung der personenbezogenen Daten muss für diese Zwecke erforderlich sein. Die Formulierung orientiert sich an der bereichsspezifischen Regelung des § 95 Absatz 2 Satz 1 des Telekommunikationsgesetzes zur Verwendung von Telekommunikationsbestandsdaten durch die Dienstanbieter. Soweit die verantwortliche Stelle für die Eigenwerbung oder eigene Markt- oder Meinungsforschung die Berufs-, Branchen- oder Geschäftsbezeichnung, den Namen, Titel, akademischen Grad, die Anschrift oder das Geburtsjahr verwenden will, muss sie diese Daten beim Betroffenen erhoben haben und zwar nach § 28 Absatz 1 Satz 1 Nummer 1. Die Regelung verlangt keine Kompletterhebung der genannten Daten. Die verantwortliche Stelle kann auf Daten verzichten, z. B. die Berufsbezeichnung oder das Geburtsjahr. Will sie diese jedoch für Zwecke der Eigenwerbung oder eigenen Markt- oder Meinungsforschung verwenden, muss sie die Daten beim Betroffenen erheben. Es ist also nicht zulässig, ein Datum beim Betroffenen zu erheben und die weiteren genannten Daten aus allgemein zugänglichen Quellen zu erheben und nach Absatz 3 Satz 3 hinzuzuspeichern. Eine gesetzliche Erlaubnis ist insofern gerechtfertigt, weil dem Betroffenen die verantwortliche Stelle durch die Erhebung der Daten im Rahmen der Zweckbestimmung eines rechtsgeschäftlichen Schuldverhältnisses oder rechtsgeschäftsähnlichen Schuldverhältnisses bekannt ist und der Betroffene auch damit rechnen kann, dass ihm die verantwortliche Stelle Werbung für weitere eigene Angebote der verantwortlichen Stelle zukommen lässt oder im Interesse der Fortsetzung des bestehenden rechtsgeschäftlichen- oder rechtsgeschäftsähnlichen Schuldverhältnisses 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 Absatz 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 Absatz 3 Satz 2 Nummer 1 ist hingegen die Verwendung, die nicht der eigenen Markt- oder Meinungsforschung oder Zwecken der Werbung dient, die nicht eigene Angebote betreffen. Insoweit rechnet der Betroffene nicht damit, dass die verantwortliche Stelle seine personenbezogenen Daten, die sie im Rahmen eines rechtsgeschäftlichen- oder rechtsgeschäftsähnlichen Schuldverhältnisses erhoben hat, ohne weiteres Zutun des Betroffenen auch dazu verwendet, sie an weitere Dritte zu veräußern oder zur Verfügung zu stellen, damit diese an den Betroffenen mit ihren Angeboten herantreten.

Nach dem Absatz 3 Satz 2 Nummer 2 muss es sich um Werbung, Markt- oder Meinungsforschung gegenüber freiberuflich oder gewerblich Tätigen handeln. Die Verwendung der personenbezogenen Daten muss für diese Zwecke erforderlich sein und sie muss sich auf die Geschäftsadresse der Betroffenen beziehen. Letzteres soll verhindern, dass freiberuflich oder gewerblich Tätige in ihrer Eigenschaft als Privatperson an ihre private Adresse Werbung erhalten, die als Geschäftswerbung deklariert wird. Geschäftliche Werbung, Markt- und Meinungsforschung unterliegt dem Bundesdatenschutzgesetz nur dann, wenn die dabei verwendeten Daten z. B. aufgrund der Firmierung oder geringen Größe eines Unternehmens einer bestimmten oder bestimmbaren Person zuordenbar sind und nach § 3 Absatz 1 personenbezogene Daten sind. Für weite Bereiche der geschäftlichen Werbung trifft dies nicht zu. Insoweit besteht eine unterschiedliche Behandlung zum Teil vergleichbarer Unternehmen in Bezug auf geschäftliche Werbung. Sie rechtfertigt, bei solchen freiberuflich oder gewerblich Tätigen keine Einwilligung vorzusehen und damit die

unterschiedliche Behandlung gegenüber den Unternehmen zu erweitern, die bezüglich geschäftlicher Werbung keinen Anforderungen des Bundesdatenschutzgesetzes unterliegen, sondern weiterhin eine gesetzliche Erlaubnis vorzusehen. Auf diese Weise wird das informationelle Selbstbestimmungsrecht der betroffenen freiberuflich oder gewerblich Tätigen auch nicht übermäßig eingeschränkt, da ihnen weiterhin das Widerspruchsrecht erhalten bleibt. Eine gesetzliche Erlaubnis ist auch gerechtfertigt, weil Werbung, Markt- und Meinungsforschung im geschäftlichen Verkehr zwischen Unternehmen mit Verbraucherwerbung nicht vergleichbar ist. Sie wird von den betroffenen gewerblich oder freiberuflich Tätigen weniger als ein Eingriff in ihr informationelles Selbstbestimmungsrecht wahrgenommen als - im Übermaß - ein Eingriff in ihren eingerichteten und ausgeübten Gewerbebetrieb. Werbung, Markt- und Meinungsforschung verfolgt insoweit einen anderen Zweck als bei Verbrauchern. Bei gewerblich oder freiberuflich Tätigen erleichtert sie die Marktorientierung, z. B. hinsichtlich der Angebote und Preise von Wettbewerbern, und eröffnet Marktchancen und Investitionsanreize, z. B. bei neuen Entwicklungen. Daher ist bei gewerblich oder freiberuflich Tätigen potentiell von einem größeren Interesse am Erhalt der mit der Werbung verbundenen Informationen auszugehen als allgemein bei Verbrauchern, die zueinander nicht in Konkurrenz stehen. Vor dem Hintergrund der andersartigen Qualifikation und dem damit verbundenen geringeren Interesse gewerblich oder freiberuflich Tätiger, die Herkunft auf ihre - in aller Regel allgemein zugängliche - Geschäftsadresse bezogene Werbung zurückzuverfolgen, kann von einer Kennzeichnung der Herkunft abgesehen werden. Die Regelung zielt auf eine Entlastung der in diesem Bereich besonders stark vertretenen spezialisierter kleinerer und mittlerer Unternehmen.

Nach Absatz 3 Satz 2 Nummer 3 muss die Verwendung für Zwecke der Spendenwerbung einer verantwortlichen Stelle erfolgen, wenn Spenden an diese gemäß § 10b Absatz 1 und § 34g des Einkommenssteuergesetzes steuerbegünstigt sind. Insofern wird der bestehende Zustand beibehalten. Zu den steuerbegünstigten Zwecken gehören u. a. gemeinnützige, mildtätige und kirchliche Zwecke nach den §§ 52 bis 54 der Abgabenordnung. Die Ausnahme ist beschränkt auf die Verwendung 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 Absatz 4 Satz 1 machen kann. Im Hinblick auf das öffentliche Interesse, das an Empfängern steuerbegünstigter Spenden 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 Absatz 3 Satz 3 darf die verantwortliche Stelle für Zwecke der Werbung für eigene Angebote oder der eigenen Markt- oder Meinungsforschung zu den in Satz 2 Nummer 1 genannten Daten (Berufs-, Branchen- oder Geschäftsbezeichnung, Name, Titel, akademischer Grad, Anschrift, Geburtsjahr), die sie beim Betroffenen nach Absatz 1 Satz 1 Nummer 1 erheben muss, weitere Daten hinzuspeichern. Die Beschränkung auf das „hinzuspeichern“ stellt klar, dass die verantwortliche Stelle die weiteren Daten gestützt auf eine andere Befugnis rechtmäßig erhoben, z. B. nach Absatz 1 Satz 1 Nummer 3, oder rechtmäßig übermittelt bekommen haben muss. Absatz 3 Satz 3 ist keine eigene Erhebungs- oder Übermittlungsbefugnis. Absatz 3 Satz 3 soll es der verantwortlichen Stelle ermöglichen, einen eigenen Datenbestand, der direkt beim Betroffenen erhoben wurde, für Zwecke der Eigenwerbung oder der eigenen Markt- oder Meinungsforschung zu selektieren, um die bestehenden Kunden gezielter ansprechen zu können. Die Transparenz der Datenverwendung bleibt dabei weitgehend gewahrt, da der Datenverwender im Rahmen der Eigenwerbung oder eigenen Markt- oder Meinungsforschung für den Betroffenen erkennbar bleibt, z. B. zur Wahrnehmung des Widerspruchsrechts nach Absatz 4 Satz 1.

Nach Absatz 3 Satz 4 ist die Nutzung für Zwecke der Werbung, Markt- oder Meinungsforschung zudem zulässig, soweit sie zusammen mit Eigenwerbung oder eigener Markt- oder Meinungsforschung nach Satz 2 Nummer 1 erfolgt, aber auch sofern sie zusammen

mit der Durchführung eines rechtsgeschäftlichen Schuldverhältnisses oder rechtsgeschäftsähnlichen Schuldverhältnisses, z. B. im Rahmen der Zusendung der Leistung oder der Rechnung erfolgt. Die Nutzung für „Zwecke der Werbung, Markt- oder Meinungsforschung“ verdeutlicht, dass es sich auch um Fremdwerbung oder fremdbezogene Markt- oder Meinungsforschung handeln kann. Die Beschränkung auf „Nutzung“ stellt allerdings klar, dass die verantwortliche Stelle die personenbezogenen Daten, die sie hierfür drittbezogen nutzen will, selbst nach Absatz 1 Satz 1 Nummer 1 erhoben haben muss. Dies gilt auch mittelbar, soweit auf Satz 2 Nummer 1 Bezug genommen wird. Absatz 3 Satz 4 ist keine eigene Erhebungs- oder Übermittlungsbefugnis. Erlaubt wird damit so genannte „Beipackwerbung“, die insbesondere im Unternehmensverbund und in Konzernen von Bedeutung, hierauf aber nicht beschränkt ist. Die Regelung zielt auch auf eine Entlastung spezialisierter kleinerer und mittlerer Unternehmen. Wie in Satz 3 bleibt die Transparenz der Datennutzung weitgehend gewahrt, da der Datennutzer im Rahmen der Eigenwerbung, der eigenen Markt- oder Meinungsforschung oder der Durchführung des eigenen rechtsgeschäftlichen Schuldverhältnisses oder rechtsgeschäftsähnlichen Schuldverhältnisses für den Betroffenen erkennbar bleibt, z. B. zur Wahrnehmung des Widerspruchsrechts nach Absatz 4 Satz 1. Insoweit erübrigt sich auch eine Herkunftskennzeichnung. Eine weitere tatsächliche Eingrenzung in der Praxis besteht darin, dass der Betroffene zwar Fremdwerbung erhält, diese aber dem gleichzeitig in Erscheinung tretenden Datennutzer zuordnet. Für den Betroffenen ist transparent, wer seine personenbezogenen Daten für die Fremdwerbung kommerziell nutzt. Dies wirkt sich potentiell negativ für den Datennutzer aus. Packt er z. B. zu viel, unerwünschte oder qualitativ minderwertige Werbung bei, droht ihm ein Vertrauensschaden bei dem Betroffenen oder gar dessen Widerspruch nach Absatz 4 Satz 1. Daher ist nicht zu erwarten, dass sich auf die Ausnahme des Satz 4 gestützte missbräuchliche Geschäftsformen etablieren.

Nach Absatz 3 Satz 5 ist die Verwendung personenbezogener Daten nach den Sätzen 2 bis 4 unbeschadet der dortigen Voraussetzungen nur zulässig, soweit schutzwürdige Interessen des Betroffenen nicht entgegenstehen. Satz 5 gewährleistet, wie die bestehende Regelung des § 28 Absatz 3 Satz 1 Nummer 3 und § 28 Absatz 1 Satz 1 Nummer 2, die notwendige Flexibilität für die gesetzlichen Erlaubnistatbestände, im Einzelfall zu abweichenden Ergebnissen zu gelangen, da anders als bei Satz 1 keine Einwilligung des Betroffenen als Manifestation seiner informationellen Selbstbestimmung bekannt ist und zugrunde gelegt werden kann.

Absatz 3 Satz 6 enthält die im Bundesdatenschutzgesetz übliche Zweckbindung, wie sie sich unter anderem in Absatz 5 Satz 1 für Dritte befindet.

Nach Absatz 3a Satz 1 unterliegt die Einwilligung der allgemeinen Form des § 4a Absatz 1 Satz 3 des Bundesdatenschutzgesetzes, d.h. die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soweit eine andere Form angemessen ist, geht es um ein Abweichen von der Erklärungsform. Es bedarf jedoch weiterhin einer ausdrücklichen, das Einverständnis des Betroffenen dokumentierenden Erklärung. Eine konkludente, stillschweigende oder gar mutmaßliche Einwilligung reicht daher nicht aus. Wann besondere Umstände des Einzelfalls vorliegen, kann nicht abstrakt dargestellt werden, sondern ist abhängig von den spezifischen Umständen der Verarbeitung. Die grundsätzlich vorgesehene Schriftform soll ohne Zweifel dokumentieren, dass der Betroffene sich damit einverstanden erklärt hat, dass seine personenbezogenen Daten auch für fremde Zwecke der Werbung oder Markt- oder Meinungsforschung verwendet werden können. Die Schriftform soll dabei ermöglichen, etwaige Grenzen der Einwilligung (z. B. Übermittlung nur innerhalb des Konzerns oder nur an bestimmte Dritte oder nur Nutzung aber keine Übermittlung) nachzuvollziehen. Zugleich soll die Schriftform dem Betroffenen die Bedeutung der Einwilligung vor Augen führen, da die hierdurch ermöglichte Übermittlung an Dritte es ihm erschwert, von seinem Widerrufsrecht Gebrauch zu machen. Wird die Einwilligung in anderer Form als der Schriftform erteilt, hat die verantwortliche Stelle dem Betroffenen den Inhalt der Einwilligung schriftlich zu bestätigen, damit er kontrollieren kann, ob die verantwortliche Stelle die erteilte Einwilligung

korrekt dokumentiert hat. Einer schriftlichen Bestätigung bedarf es nicht,, wenn die verantwortliche Stelle bestimmte technische Vorkehrungen trifft, die sich in dieser Form bereits in § 94 des Telekommunikationsgesetzes und § 13 Absatz 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 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 Absatz 1 Satz 4 sieht insoweit lediglich vor, dass die Einwilligung besonders hervorgehoben werden muss, z. B. durch eine auffällige typographische Gestaltung (größere Schrifttype, Fettdruck, Umrahmung). Satz 2 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. Die Bundesregierung wird die Auswirkungen des Formerfordernisses aufmerksam beobachten und drei Jahre nach Inkrafttreten ergebnisoffen evaluieren.

Absatz 3b sieht vor, dass die verantwortliche Stelle sich die Einwilligung des Betroffenen nach Absatz 3 Satz 1 in eine Verwendung seiner personenbezogenen Daten, die nicht 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 gleichwertigen vertraglichen Gegenleistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist. Die Formulierung lehnt sich damit an die bisherigen bereichsspezifischen Kopplungsverbote in § 95 Absatz 5 des Telekommunikationsgesetzes und in § 12 Absatz 3 des Telemediengesetzes an und ergänzt diese durch die Wörter „ohne die Einwilligung“. Erfasst werden soll auf diese Weise die Konstellation, dass die marktbeteiligten Unternehmen für sich genommen jeweils keine marktbeherrschende Stellung besitzen und dem Betroffenen daher ein Zugang zu gleichwertigen vertraglichen Leistungen an sich in zumutbarer Weise möglich ist, z. B. durch Absprachen unter den marktbeteiligten Unternehmen, aber marktweit immer nur, wenn er seine Einwilligung erteilt. Umgekehrt formuliert: Ein Zugang ist nicht in zumutbarer Weise möglich, wenn er nur mit Einwilligung nach Absatz 3 Satz 1 möglich ist.

Die Änderungen in Absatz 4 Satz 1 und 3 sind redaktionelle Anpassungen an die Formulierung des Absatzes 3.

Die Änderung in Satz 2 und der neue Satz 4 bezwecken eine Stärkung des Widerspruchsrechts der Betroffenen. Nach Satz 1 besitzen die Betroffenen die Möglichkeit, der Verarbeitung oder Nutzung ihrer personenbezogenen Daten für Zwecke der Werbung, Markt- oder Meinungsforschung zu widersprechen. Nach dem bisherigen Satz 2 ist der Betroffene hierüber erst bei der werblichen Ansprache zu unterrichten, d.h. nach einer Verarbeitung oder Nutzung seiner personenbezogenen Daten für diese Zwecke. Satz 2 sieht vor, dass der Betroffene bei der Begründung eines rechtsgeschäftlichen Schuldverhältnisses oder rechtsgeschäftsähnlichen Schuldverhältnisses künftig auch zu diesem Zeitpunkt auf sein Widerspruchsrecht hinzuweisen ist, um bereits zu diesem Zeitpunkt, vor der Verarbeitung oder Nutzung zu Zwecken der Werbung, Markt- oder Meinungsforschung, Kenntnis von dem Widerspruchsrecht zu erlangen und gegebenenfalls unmittelbar Gebrauch zu machen. Hieran anknüpfend sieht Satz 4 vor, dass für den Widerspruch keine strengere Form verlangt werden darf als für die Begründung des rechtsgeschäftlichen Schuldverhältnisses oder rechtsgeschäftsähnlichen Schuldverhältnisses. Derzeit ist teilweise zu beobachten, dass zwar mit geringen Formerfordernissen ein Vertragsabschluss möglich

ist, z. B. durch elektronische Erklärung im Internet, an den Widerspruch dagegen höhere Anforderungen gestellt werden, z. B. die Schriftform.

Die Änderung in Absatz 9 Satz 4 ist eine redaktionelle Anpassung an die Verschiebung des Erlaubnistatbestandes des bestehenden Absatzes 3 Satz 1 Nummer 2 zu Absatz 2 Nummer 2 Buchstabe b.

Zu Nummer 6 (§ 29)

Die Änderungen in § 29 Absatz 1 und 2 sind notwendige redaktionelle Änderungen und Folgeänderungen, durch die die Änderungen in § 28 Absatz 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 Absatz 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 Absatz 3 Satz 1 Nummer 3. Die Vorschrift in Absatz 2 Satz 2 sieht vor, dass die Änderungen in § 28 Absatz 3 bis 3b auch für die geschäftsmäßige Übermittlung im Rahmen der Zwecke nach § 29 Absatz 1 gelten.

Zu Nummer 7 (§ 33 Absatz 2 Satz 1 Nummer 8 Buchstabe b)

Es handelt sich um eine Folgeänderung der unter Ziffer 6 vorgesehenen Änderung.

Zu Nummer 8 (§ 42a)

Die Vorschrift enthält eine Informationspflicht für nichtöffentliche Stellen und ihnen datenschutzrechtlich gleichgestellte öffentlich-rechtliche Wettbewerbsunternehmen. Sonstige öffentliche Stellen werden nicht einbezogen. Die Informationspflicht besteht, wenn bestimmte besonders sensible personenbezogene Daten Dritten unrechtmäßig zur Kenntnis gelangen und schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen. Die Vorschrift knüpft an einen Vorschlag der Kommission der Europäischen Gemeinschaften zur Änderung der Richtlinie 2002/58/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 nach Satz 1 Nummer 1 bis 4 auf besonders sensible personenbezogene Daten aus dem Verfügungsbereich der verantwortlichen Stelle begrenzt. Hierzu gehören besondere Arten personenbezogener Daten nach § 3 Absatz 9, personenbezogene Daten, die einem Berufsgeheimnis unterliegen, personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen und personenbezogene Daten zu Bank- oder Kreditkartenkonten. Für Bestandsdaten nach § 3 Nummer 3 des Telekommunikationsgesetzes und Verkehrsdaten nach § 3 Nummer 30 des Telekommunikationsgesetzes sowie Bestandsdaten nach § 14 des Telemediengesetzes und Nutzungsdaten nach § 15 des Telemediengesetzes ist eine bereichsspezifische Regelung im Telekommunikationsgesetz und im Telemediengesetz vorgesehen.

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 Absatz 1 Satz 1 feststellt, dass bei der verantwortlichen Stelle gespeicherte personenbezogene Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten nach § 3 Absatz 8 Satz 2 zur Kenntnis gelangt sind und 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 verantwortliche Stelle hat – unter Einbeziehung des Beauftragten für den Datenschutz nach § 4g Absatz 1 Satz 1 – in diesem Fall sowohl die zuständige Datenschutzaufsichtsbehörde als auch die Betroffenen zu informieren. Bei nichtöffentlichen 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 nach Satz 1 sowohl gegenüber der Aufsichtsbehörde als auch den Betroffenen unverzüglich, d.h. nach der Legaldefinition des § 121 des Bürgerlichen Gesetzbuchs ohne schuldhaftes Zögern, erfolgen. Satz 2 sieht dabei eine Differenzierung vor. Während die Benachrichtigung der Aufsichtsbehörden aufgrund ihrer Verschwiegenheitspflicht auch vor der Beseitigung von Datensicherheitslücken und im Falle laufender Strafverfolgungsmaßnahmen erfolgen muss, stellt Satz 2 für die Benachrichtigung der Betroffenen 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 die 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 nach Satz 3 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 nach Satz 4 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 direkten Benachrichtigung der Betroffenen tritt mit deren Inhalt nach Satz 5 eine Information der Öffentlichkeit. Dies wird durch Anzeigen, die mindestens eine halbe Zeitungsseite umfassen, in mindestens zwei bundesweit erscheinenden Tageszeitungen sichergestellt.

Satz 6 enthält ein flankierendes strafrechtliches Verwertungsverbot, wie es auch in anderen Vorschriften, z. B. § 97 Absatz 1 Satz 2 der Insolvenzordnung, vorgesehen ist. Danach dürfen die Benachrichtigung bzw. die darin enthaltenen Informationen in einem Strafverfahren oder in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen den Benachrichtigungspflichtigen oder einen seiner Angehörigen nach § 52 Absatz 1 der Strafprozessordnung nur mit Zustimmung des Benachrichtigungspflichtigen verwendet werden. Auf diese Weise wird das Spannungsverhältnis verfassungskonform aufgelöst, dass der Betroffene entweder sich selbst bezichtigt oder nach § 43 Absatz 2 Nummer 7 sich ordnungswidrig verhält. Dabei ist zu berücksichtigen, dass eine Selbstbezichtigung bei juristischen Personen nicht der Regelfall ist, für einen Teil der betroffenen Unternehmen (z. B. Ein-Mann-GmbH) aber jedenfalls tatbestandlich in Betracht kommt.

Zu Nummer 9 (§ 43)

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

In § 43 Absatz 1 werden drei neue Bußgeldtatbestände aufgenommen: Nach der Nummer 2a handelt die speichernde Stelle ordnungswidrig, wenn sie entgegen § 10 Absatz 4 Satz 3 bei einem automatisierten Abrufverfahren nicht gewährleistet, dass die Übermittlung personenbezogener Daten durch Abruf durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann. Die Übermittlung personenbezogener Daten durch Abruf, die vor allem bei größeren Datenbeständen und einer größeren Anzahl von Übermittlung angewandt wird, ist aus Sicht des Rechts auf informationelle Selbstbestimmung gefahrgeneigt, weil die übermittelnde Stelle die personenbezogenen Daten lediglich zum Abruf bereitstellt, vor der Übermittlung durch Abruf jedoch im Regelfall keine weitere Prüfung der Zulässigkeit vornimmt. Diese fehlende Vorabprüfung wird datenschutzrechtlich unter anderem dadurch aufgefangen, dass nachträglich durch Stichprobenverfahren gewährleistet wird, dass die übermittelnde Stelle die Zulässigkeit des Abrufs überprüfen kann. Aus Sicht der Aufsichtpraxis wird dieses Erfordernis des Öfteren nicht beachtet und kann bislang mangels Bußgeldbewehrung auch nur unzureichend gegen die verantwortliche Stelle durchgesetzt werden. Nach Nummer 2b handelt der Auftraggeber ordnungswidrig, wenn er entgegen § 11 Absatz 2 Satz 2 den Auftrag nicht schriftlich erteilt oder nicht die vorgegebenen Festlegungen hinsichtlich der Datenerhebung oder -verwendung sowie die technischen und organisatorischen Maßnahmen und Unterauftragsverhältnisse festlegt. Die Aufsichtspraxis weist darauf hin, dass ein vollständiger schriftlicher Auftrag die Ausnahme ist. Die Bußgeldbewehrung soll es der Praxis ermöglichen, die gesetzlich vorgesehenen Rahmenbedingungen der Auftragsdatenverarbeitung besser durchsetzen zu können. Nach Nummer 3a handelt die verantwortliche Stelle ordnungswidrig, die entgegen § 28 Absatz 4 Satz 4 für den Widerspruch des Betroffenen, seine personenbezogenen Daten für Zwecke der Werbung, Markt- oder Meinungsforschung zu verwenden, eine strengere Form verlangt als für die Begründung des rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses, in dessen Rahmen diese Daten erhoben werden.

In § 43 Absatz 2 werden zwei neue Bußgeldtatbestände aufgenommen und ein bestehender Bußgeldtatbestand geändert: In Nummer 5 wird die Angabe", indem er sie an Dritte weitergibt" gestrichen. Dadurch wird die zweckwidrige Nutzung in den dort genannten Fällen allgemein bußgeldbewehrt und nicht länger auf den Fall beschränkt, dass die zweckwidrige Nutzung in der Weitergabe an Dritte besteht. Nach Nummer 5a handelt die verantwortliche Stelle ordnungswidrig, wenn sie entgegen § 28 Absatz 4 Satz 1, d.h. trotz des Widerspruchs eines Betroffenen, seine personenbezogenen Daten für Zwecke der

Werbung, der Markt- oder Meinungsforschung verarbeitet oder nutzt. Nach der neuen Nummer 7 handelt schließlich die Stelle ordnungswidrig, die entgegen § 42a Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht.

Der derzeitige Bußgeldrahmen für Verstöße gegen den Bußgeldkatalog des § 43 Absatz 1 beträgt 25 000 Euro, für Verstöße gegen den Bußgeldkatalog des § 43 Absatz 2 beträgt er 250 000 Euro. Der Bußgeldrahmen geht zurück auf die Überarbeitung der Straf- und Bußgeldvorschriften im Jahre 2001. Seitdem hat sich die Informationstechnik weiter verbreitet und durchdringt zunehmend auch wirtschaftlich relevante Bereiche des alltäglichen Lebens. Damit einher geht eine wachsende wirtschaftliche 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 Absatz 2 des Telekommunikationsgesetzes und auch der Bußgeldrahmen des Entwurfs für ein Gendiagnostikgesetz in § 26 Absatz 2 einen Bußgeldrahmen von 300 000 Euro vor. Der Bußgeldrahmen für Verstöße gegen materielle Vorschriften im Bußgeldkatalog des § 43 Absatz 2 ist daher moderat von 250 000 Euro auf 300 000 Euro anzupassen. Zugleich wird der Bußgeldrahmen für Verstöße gegen Verfahrensvorschriften im Bußgeldkatalog des § 43 Absatz 1 von 25 000 Euro auf 50 000 Euro 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 Sätze 2 und 3 treten ergänzend zu der Verschärfung des Bußgeldrahmens. Sie stellen sicher, dass Tätern 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 Absatz 3 Satz 2, 3 des Telekommunikationsgesetzes, 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 10 (§ 47)

Die Vorschrift sieht eine Übergangsvorschrift von 36 Monaten vor mit Blick auf die neuen Anforderungen an die Erhebung personenbezogener Daten. Mit dem Stichtag 1. Juli 2012 gelten die neuen Anforderungen. Die betroffenen verantwortlichen Stellen werden daher bereits vor dem Inkrafttreten zum 1. Juli 2012 beginnen müssen, ihre Datenerhebung schrittweise umzustellen.

Zu Artikel 3

Nummer 1 (§ 11 Absatz 3)

Es handelt sich um eine redaktionelle Folgeänderung zu Nummer 2.

Nummer 2 (§ 12 Absatz 3)

Es handelt sich um eine Änderung des Telemediengesetzes, die aus der Einführung eines entsprechenden Kopplungsverbotes im Bundesdatenschutzgesetz folgt. Bisher besteht das eingeschränkte Kopplungsverbot nach § 12 Absatz 3 des Telemediengesetzes als eine Spezialregelung für Telemedienanbieter. Dafür besteht kein Anlass mehr, denn die allgemeinen Datenschutzregeln gelten nach § 12 Absatz 4 des Telemediengesetzes auch für Telemedienanbieter.

Nummer 3 (§ 15a)

Die Vorschrift des § 42a des Bundesdatenschutzgesetzes soll bereichsspezifisch auch für Bestands- und Nutzungsdaten nach den §§ 14, 15 des Telemediengesetzes Anwendung finden.

Nummer 4 (§ 16 Absatz 2)

Es handelt sich um eine Folgeänderung zu Nummer 2. Dabei entfällt die Bußgeldbewehrung des Kopplungsverbots, da § 28 Absatz 3b (neu) des Bundesdatenschutzgesetzes nicht bußgeldbewehrt ist.

Zu Artikel 4

Nummer 1 (§ 93 Absatz 3)

Die Vorschrift des § 42a des Bundesdatenschutzgesetzes soll bereichsspezifisch auch für Bestands- und Verkehrsdaten nach § 3 Nummer 3 und 30 des Telekommunikationsgesetzes Anwendung finden.

Nummer 2 (§ 95 Absatz 5)

Es handelt sich um eine Änderung des Telekommunikationsgesetzes, die aus der Einführung eines entsprechenden Kopplungsverbotes im Bundesdatenschutzgesetz folgt. Bisher besteht das eingeschränkte Kopplungsverbot nach § 95 Absatz 5 des Telekommunikationsgesetzes als eine Spezialregelung für Anbieter von Telekommunikationsdiensten. Aus der Einführung eines Kopplungsverbotes im Bundesdatenschutzgesetz ergibt sich die Notwendigkeit, das bereits bestehende Kopplungsverbot im Telekommunikationsgesetz an die neue Regelung im Bundesdatenschutzgesetz anzupassen, um klarzustellen, dass beide Kopplungsverbote inhaltlich deckungsgleich sind und sich lediglich an unterschiedliche Adressaten, nämlich auf der einen Seite an die nichtöffentlichen Stellen im Sinne des Bundesdatenschutzgesetz und auf der anderen Seite an die Diensteanbieter im Sinne des Telekommunikationsgesetzes, richten. Es wird klargestellt, dass das Kopplungsverbot greift, wenn ein anderer Zugang zu einem Telekommunikationsdienst ohne Einwilligung nicht oder nicht in zumutbarer Weise möglich ist.

Zu Artikel 5

Das Bundesdatenschutzgesetz ist zuletzt im Jahre 2003 bekannt gemacht worden. Da es seither mehrfach und in größerem Umfang geändert worden ist, erlaubt Artikel 5 eine Neubekanntmachung.

Zu Artikel 6

Die Vorschrift regelt das Inkrafttreten des Gesetzes.

Artikel 1 des Gesetzes, das Datenschutzauditgesetz, soll am Tag nach der Verkündung in Kraft treten, damit sich der Datenschutzauditausschuss frühzeitig konstituieren und mit der Erarbeitung und dem Beschluss von Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit als Grundlage für die Kennzeichnung mit dem Datenschutzauditsiegel beginnen kann. Es soll weiterhin frühzeitig ermöglicht werden, dass sich private Kontrollstellen gründen und zulassen. Schließlich sollen Bund und Länder frühzeitig in die Lage versetzt werden, von der Ermächtigung zum Erlass von als notwendig erachteter Rechtsverordnungen Gebrauch zu machen. Die Möglichkeit, ein Datenschutzaudit nach dem Datenschutzauditgesetz durchzuführen, soll nach § 20 Datenschutzauditgesetz aufgrund dieser notwendigen Vorbereitungsmaßnahmen erst ab dem 1. Juli 2010 möglich sein.

Artikel 2, 3 und 4 des Gesetzes sollen am 1. Juli 2009 in Kraft treten. Aufgrund der Übergangsvorschrift in Artikel 2 Nummer 10 verbleiben den betroffenen verantwortlichen Stellen damit drei Jahre, ihre Datenbestände den neuen Anforderungen anzupassen und Daten nach der neuen Fassung des § 28 des Bundesdatenschutzgesetzes zu erheben.