

Stellungnahme

Stellungnahme zum Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes und zur Regelung des Datenschutzaudits

03.11.2008

Seite 1

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.200 Unternehmen, davon 900 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Anbieter von Software, IT-Services und Telekommunikationsdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien. Der BITKOM setzt sich insbesondere für bessere ordnungspolitische Rahmenbedingungen, eine Modernisierung des Bildungssystems und eine innovationsorientierte Wirtschaftspolitik ein.

Bundesverband
Informationswirtschaft,
Telekommunikation und
neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: +49.30.27576-0
Fax: +49.30.27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner
Dr. Kai Kuhlmann
Bereichsleiter Electronic
Business-Recht
Tel.: +49.30.27576-131
Fax: +49.30.27576-139
k.kuhlmann@bitkom.org

Präsident
Prof. Dr. Dr. h.c. mult.
August-Wilhelm Scheer

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Stellungnahme

Änderung BDSG und Regelung Datenschutzaudit

Seite 2

Inhalt

1	Sachgerechter Interessenausgleich	3
2	§§ 28 und 29 BDSG: Streichung des Listenprivilegs und Einführung eines Opt-In für die Datennutzung zu Marketingzwecken	4
2.1	Auswirkungen der Einführung einer generellen Opt-In-Regelung ohne Erhalt des Listenprivilegs für schriftliche Werbung	4
2.2	Verfassungsrechtliche Bedenken.....	5
2.3	Alternative zur Streichung des Listenprivilegs: Nutzung des Listenprivilegs bei freiwilligem Datenschutzaudit und Gütesiegel	5
2.4	§ 28 Absatz 3 Nr. 1 BDSG, Verarbeitung oder Nutzung für Zwecke der verantwortlichen Stelle	6
2.5	Ausgestaltung des Opt-in durch § 28 Abs. 3a BDSG, Einwilligung.....	7
2.6	Koppelungsverbot durch § 28 Abs. 3b BDSG.....	7
3	Stärkung des betrieblichen Datenschutzbeauftragten, § 4f Abs. 3 Satz 5e.....	8
4	§ 44 a BDSG, Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten.....	8
5	§ 47, Übergangsregelung	9
6	Datenschutzauditgesetz	9
6.1	Bedarf und Nutzen	10
6.2	§ 1, Maßstab und Gegenstand des Datenschutzaudits	11
6.2.1	Auditgegenstand	11
6.2.2	Maßstab der Auditierung	12
6.2.3	Freiwilligkeit des Audits	13
6.3	Verfahren der Auditierung, §§ 1 - 6	13
6.4	Dauer der Berechtigung, das Datenschutzauditsiegel zu verwenden	14
6.5	Zuständigkeit, § 2.....	15
6.6	§ 3 Satz 2, Einbeziehung des betrieblichen Datenschutzbeauftragten	15
6.7	§ 4, Zulassung der Kontrollstellen und Entziehung der Zulassung.....	15
6.8	§ 5, Pflichten der Kontrollstelle, Kontrahierungszwang	15
6.9	§ 6, Überwachung der Kontrollstellen durch die zuständigen Behörden.....	16
6.10	§ 8, Kennzeichnung mit dem Datenschutzauditsiegel, Verzeichnisse.....	17
6.11	§ 9, Anforderungen an Kontrollstellen.....	17
6.12	§ 12, Mitglieder des Datenschutzauditausschusses, Berufung und Vorschlagsrecht.....	17
6.13	§ 17 Bußgeldvorschrift	18
6.14	§ 18, Strafvorschrift	18
6.15	§ 19, Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten.....	18
6.16	Sonstiges.....	18

Stellungnahme

Änderung BDSG und Regelung Datenschutzaudit

Seite 3

Datenschutz ist eine Herausforderung der ITK-Branche, in der sich die Bedürfnisse der Verbraucher mit den Interessen der Unternehmen decken. Kein Unternehmen kann es sich leisten, dass seine Kunden das Vertrauen in das Unternehmen, dessen Produkte oder den Vertriebsweg verlieren. An der Lösung der aktuellen Probleme möchte sich der BITKOM daher aktiv und konstruktiv beteiligen. Wir hoffen, mit unserer Einschätzung des Gesetzentwurfs zur Findung sachgerechter Regelungen beitragen zu können. Auch für den weiteren Dialog stehen wir gerne zur Verfügung.

1 Sachgerechter Interessenausgleich

Der maßgebliche Auslöser für den vorliegenden Gesetzentwurf waren mehrere Fälle von eklatanten Datenschutzverstößen in der Wirtschaft, die – sehr nachvollziehbar – zu einer erheblichen Verunsicherung der Bürger geführt haben.

BITKOM ist der Meinung, dass der Verunsicherung der Bürger unbedingt entgegengewirkt werden muss. Die zu treffenden Maßnahmen dürfen aber nicht zugleich dem Direktmarketing als Werbeform die Grundlage entziehen und damit immensen wirtschaftlichen Schaden zur Folge haben.

Allen Vorfällen der letzten Monate ist gemeinsam, dass sie nicht im rechtsfreien Raum stattgefunden haben, sondern dass vorsätzlich und in krimineller Weise gegen geltendes Recht verstoßen worden ist. Bei der derzeitigen politischen Diskussion um neue Vorschriften im Datenschutz geht es also nicht um die Schließung etwaiger Regelungslücken oder die Beseitigung von Lücken bei der Umsetzung und des Vollzugs der staatlichen Datenschutzaufsicht, sondern um den einseitigen Ausbau des Verbraucherschutzes. Diese Sichtweise als Instrument des Verbraucherschutzes greift aber zu kurz, weil sie den verfassungsrechtlichen Grundlagen nicht gerecht wird, wonach das Grundrecht auf informationelle Selbstbestimmung allen Menschen zusteht, ob Verbraucher oder nicht. Wir befürchten, dass durch die Vorschläge keinesfalls das nötige Gleichgewicht zwischen den Interessen von Kunden und Unternehmen hergestellt wird.

Es muss gegen den kriminellen Missbrauch und die schwarzen Schafe vorgegangen werden – aber dieses Vorgehen darf nicht auf Kosten derjenigen gehen, die sich datenschutzkonform verhalten haben und auch zukünftig verhalten werden. Wir appellieren daher an das Bundesministerium des Inneren, bei den Änderungen des BDSG alle berechtigten Interessen in einen sachgerechten Ausgleich zu bringen.

Eines der Elemente, das in diesem Prozess Berücksichtigung finden muss, ist der Wert der Werbung für die Wirtschaft und den Kunden. Dieser Wert muss erhalten bleiben.

Der Wert der Werbung ist von der ganz überwiegenden Mehrheit der Bürger schon lange akzeptiert. Viele Bürger haben in der Werbung die Möglichkeit erkannt, nützliche Informationen über Produkte und Leistungen zu erhalten. Die Wirtschaft hat sich auf die Bedürfnisse der Kunden eingestellt und bietet ihm über das Direktmarketing verschiedenste Möglichkeiten, sich individuell und

Stellungnahme

Änderung BDSG und Regelung Datenschutzaudit

Seite 4

zielgenau über neue Produkte zu informieren. Mehr als 80 Prozent aller Unternehmen in Deutschland nutzen Direktmarketing. Für den Mittelstand ist Direktmarketing die einzige finanzierbare Werbeform.

Vor diesem Hintergrund möchte BITKOM seine Einschätzung zu den Gesetzesvorschlägen des Referentenentwurfs abgeben. Maßstab der Einschätzung ist dabei die gesetzgeberische Zielsetzung, vorsätzlichen Missbrauch von Daten zu verhindern und dadurch die Verbraucher zu schützen.

2 §§ 28 und 29 BDSG: Streichung des Listenprivilegs und Einführung eines Opt-In für die Datennutzung zu Marketingzwecken

Der Entwurf sieht die Abschaffung des Listenprivilegs vor. Dadurch soll die Nutzung und Übermittlung personenbezogener Daten zu Zwecken des Adresshandels zukünftig nur noch mit ausdrücklicher Einwilligung des Bürgers möglich sein. Nach Ansicht des BITKOM sollte das in den § 28 und § 29 des BDSG definierte Listenprivileg für schriftliche Werbung jedoch unbedingt erhalten bleiben (ein entsprechender Regelungsvorschlag ist unter Punkt 2.3 dargestellt).

2.1 Auswirkungen der Einführung einer generellen Opt-In-Regelung ohne Erhalt des Listenprivilegs für schriftliche Werbung

Seriöses Adressgeschäft ist für die deutsche Wirtschaft unverzichtbar. Laut dem aktuellen Direktmarketing-Monitor der Deutschen Post haben die Unternehmen in Deutschland im Jahr 2006 ca. 70 Mrd. Euro in Werbung investiert, davon ca. 32 Mrd. Euro in Direktmarketing. Am Adressgeschäft hängen weit mehr als tausend kleine, mittlere und große Unternehmen sowie Hunderttausende Arbeitsplätze; es ist somit ein wichtiger Pfeiler unserer Volkswirtschaft.

Ein generelles Opt-In würde zu einer drastischen Verringerung von Adressdaten für die Direktmarketingbranche führen. Nach ersten vorsichtigen Schätzungen würde die Generierung einer einzigen generellen Opt-In-Adresse mehr als 50 Euro kosten. Ein Wert, der durch die Nutzung der Adresse für Werbezwecke (bei Vermietung bringt eine Adresse ca. 0,13 bis 0,20 €) nicht wieder eingespielt werden könnte. Zusätzlich zu den hohen Kosten für die Umstellung der unternehmensinternen Prozesse auf ein Opt-In würde es aller Voraussicht nach Jahre dauern, bis attraktive Adressbestände mit Opt-In aufgebaut wären. Unter den oben beschriebenen Rahmenbedingungen werden Unternehmen zukünftig kaum noch bereit sein, in die Adressgenerierung zu investieren. Erschwerend kommt hinzu, dass die Vermietung von Adresslisten für den Adressinhaber ein Nebengeschäft darstellt. Die Verfügbarkeit von Opt-In-Adressen würde sich im Markt im Endeffekt dramatisch reduzieren und könnte in letzter Konsequenz eine ganze Branche gefährden.

Zudem würde das Geschäft von Dienstleistungsunternehmen im Adress- und Zielgruppenmarketing massiv leiden. In zahlreichen Branchen gäbe es große Probleme bei der Neukundengewinnung – eine hohe Anzahl von Arbeitsplätzen wäre gefährdet.

Stellungnahme

Änderung BDSG und Regelung Datenschutzaudit

Seite 5

Die Einführung einer generellen Opt-In-Regelung ohne den Erhalt des Listenprivilegs für schriftliche Werbung könnte letztlich dazu führen, dass Unternehmen und Direktmarketing-Dienstleister ihren Sitz ins Ausland verlegen und von dort aus mit nicht mehr kontrollierbaren Adresslisten Endverbraucher in Deutschland anschreiben.

Eine weitere Gefahr wäre, dass der illegale Adresshandel und der Handel aus dem Ausland an Bedeutung gewinnen könnten.

2.2 Verfassungsrechtliche Bedenken

Nach den Begründungen des Gesetzes sollen die Änderungen im BDSG dazu dienen, den kriminellen Missbrauch privater Daten in der Wirtschaft zukünftig zu unterbinden. Aus Sicht des BITKOM bestehen deshalb verfassungsrechtliche Bedenken gegen die geplante Einwilligungslösung und die Abschaffung des Listenprivilegs. Denn beide Regelungen sind für den angestrebten Zweck weder geeignet, noch erforderlich und angemessen, also unverhältnismäßig im verfassungsrechtlichen Sinne.

Im Einzelnen:

Die Eignung ist zu verneinen. Bei der Gefahr der unkontrollierten Weitergabe von Daten und Adresslisten handelt es sich nicht um eine Frage der Zustimmung des Kunden zur Weitergabe der Daten, sondern um eine Frage, die sich im Bereich der Datensicherheit eines jeden Unternehmens abspielt. Dafür ist ohne jeden Belang, ob bei einem Unternehmen eine Adressliste mit Einwilligung des Kunden oder ohne Einwilligung existiert. Mit einer Einwilligungserklärung kann demnach auch nicht verhindert werden, dass Daten von kriminell vorgehenden Personen kopiert und unberechtigter Weise verwendet werden. Die Maßnahme ist also deshalb nicht geeignet, den Zweck des Gesetzgebers überhaupt zu erreichen.

Die Einführung der Einwilligungslösung ist aber auch nicht erforderlich, da es zur Erreichung des Zwecks des Gesetzgebers mildere Mittel gibt. So wäre z.B. die Verschärfung der Aufsicht, die Kontrolle der Datenbestände auf deren Sicherheit sowie die Einführung eines Datenschutzaudits ausreichend, um die Betroffenen vor der unberechtigten Weitergabe ihrer Daten zu schützen. Die angestrebte Einwilligungslösung ist schließlich auch deshalb nicht erforderlich, weil der Bundesgerichtshof für den Schutz des Betroffenen eine sogenannte Opt-out-Lösung in seinem aktuellen Urteil zu den „Payback“-Kundenkarten als angemessen eingeordnet hat. Im Rahmen dieses Urteils hat der BGH ausgeführt, dass er eine Opt-out-Lösung als ausreichend ansieht, weil der durchschnittlich informierte und verständige Verbraucher einer vorformulierten Einwilligungserklärung die der Situation angemessene Aufmerksamkeit entgegenbringt.

2.3 Alternative zur Streichung des Listenprivilegs: Nutzung des Listenprivilegs bei freiwilligem Datenschutzaudit und Gütesiegel

BITKOM ist der Auffassung, dass es unerlässlich ist, denjenigen Unternehmen, die auf schriftliche Werbung angewiesen sind, die Möglichkeit zu geben, unter bestimmten Voraussetzungen weiterhin mit dem Listenprivileg zu arbeiten.

Stellungnahme

Änderung BDSG und Regelung Datenschutzaudit

Seite 6

Vorstellbar wäre es, die Nutzung des Listenprivilegs denjenigen Unternehmen vorzubehalten, die durch ein Gütesiegel nachweisen können, dass sie ein Datenschutzaudit, das sich auf die entsprechenden Prozesse des Direktmarketings bezieht, erfolgreich durchgeführt haben.

Schon in der Stellungnahme zu dem ersten Entwurf für ein Datenschutzauditgesetz (Oktober 2007) hat BITKOM darauf hingewiesen, dass aus Sicht der Wirtschaft ein erfolgreiches Audit mit unmittelbaren Erleichterungen und Entlastungen bei der datenschutzrechtlichen Einbettung des Unternehmens verbunden sein muss, um auf Akzeptanz und Interesse bei den Unternehmen zu stoßen. Eine dieser Erleichterungen bzw. Entlastungen könnte die Koppelung von Datenschutzaudit und Listenprivileg für schriftliche Werbung sein.

Durch die Koppelung des Listenprivilegs an ein Datenschutzaudit kann eine hohe Transparenz und Datensicherheit gewährleistet sowie die Überwachung und Kontrolle optimiert werden. Diese Koppelung würde es also ermöglichen, den „schwarzen Schafen“ das Handwerk zu legen, ohne die legalen und von der Mehrheit der Bevölkerung gewünschten Direktmarketingaktivitäten zu stark einzuschränken. Auf diese Weise könnte allen berechtigten Anliegen, also sowohl dem Schutz der Verbraucher vor illegalem Adresshandel als auch dem Interesse der Wirtschaft und der Kunden an einem effektiven Direktmarketing Rechnung getragen werden. Auch die verfassungsrechtlichen Bedenken würden dann nicht mehr greifen. Zudem könnte diese Koppelung zur Verbreitung der Auditierung ganz unmittelbar beitragen.

In dem Entwurf zur Regelung des Audits ist vorgesehen, dass ein Datenschutzauditsiegel dann vergeben wird, wenn ein Unternehmen über die Einhaltung der Gesetze hinaus Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit erfüllt. Diese Vorgehensweise halten wir für begrüßenswert und sinnvoll, wenn sektor- bzw. branchenspezifische Richtlinien erarbeitet und die jeweils betroffenen Wirtschaftskreise unmittelbar und intensiv bei der Formulierung der Richtlinien beteiligt werden.

Eine derartige Richtlinie könnte auch für diejenigen Unternehmen erarbeitet werden, die weiterhin auf Grundlage des Listenprivilegs arbeiten möchten. Dies gäbe die Möglichkeit, die erforderlichen spezifischen Anforderungen an ein datenschutzgerechtes Vorgehen festzulegen.

2.4 § 28 Absatz 3 Nr. 1 BDSG, Verarbeitung oder Nutzung für Zwecke der verantwortlichen Stelle

Nicht nur bei internationalen Konzernen besteht regelmäßig eine notwendige Aufspaltung in verschiedene Gesellschaften, die gegenüber den Kunden Leistungen erbringen (z.B. bei Spartentrennung im Bereich von Versicherungen und Banken / Bausparkassen, bei TK-Festnetz- und Mobilfunkanbietern). Die im Entwurf vorgesehene Formulierung „*Werbung für eigene Angebote der verantwortlichen Stelle*“ ist daher viel zu eng. Denn auch bei der Verbindung verschiedener gesellschaftsrechtlich selbständiger Unternehmensteile kann grundsätzlich von der Annahme ausgegangen werden, dass der Kunde an Leistungen des Gesamtunternehmens ein Interesse hat, so dass die jederzeitige Opt-out-Möglichkeit als Schutzniveau genügen sollte. BITKOM schlägt daher vor, anstatt

Stellungnahme

Änderung BDSG und Regelung Datenschutzaudit

Seite 7

der jetzigen Formulierung die Formulierung „für eigene Werbezwecke“ oder aber „Werbung für eigene Angebote und Angebote verbundener Unternehmen“ aufzunehmen.

Darüber hinaus ist Abs. 3 in einem weiteren Aspekt nach Ansicht des BITKOM zu eng gefasst. Angesichts der Zielsetzung des Entwurfs ist es nicht erforderlich, geschäftliche Korrespondenz mit werblichem Charakter in Unternehmensverbänden einzuschränken (z.B. bei vergünstigten Mitarbeiterangeboten im Konzern). Klargestellt werden sollte deshalb auf jeden Fall, dass das schutzwürdige Interesse des Betroffenen am Ausschluss der Verarbeitung und Nutzung auch dann nicht überwiegt, wenn der Betroffene in seiner dienstlichen Funktion am Arbeitsplatz angeschrieben wird.

2.5 Ausgestaltung des Opt-in durch § 28 Abs. 3a BDSG, Einwilligung

§ 28 Abs. 3a BDSG ist mit seinen Anforderungen an die Form der Einwilligung nicht praxistauglich und klammert den telefonischen Kontakt völlig aus. Daraus resultieren nicht gerechtfertigte Medienbrüche, weil nach dem telefonischen Kontakt eine schriftliche oder elektronische Einwilligung zusätzlich eingeholt werden müsste, wodurch Unternehmen mit höherem Telekommunikationsaufkommen ungerechtfertigt benachteiligt werden. BITKOM hält die Dokumentation der erklärten Einwilligung durch Mitarbeiter des Unternehmens für ausreichend, zumal das Unternehmen selbst ein erhebliches Interesse an der ordnungsgemäßen Dokumentation hat, denn im Streitfall müsste es die Einwilligung beweisen. Die Dokumentation könnte durch eine Informationspflicht in Textform ergänzt werden; die Betroffenen können ohnehin die Einwilligung jederzeit widerrufen und sind so effektiv geschützt.

Darüber hinaus ist auch im Kontext des § 28 Abs. 3a BDSG die Möglichkeit sicherzustellen, dass die Datenweitergabe in Unternehmensverbänden nicht an das vorherige Opt-in und die Voraussetzungen des Abs. 3a gebunden ist. Die Datenweitergabe ist bei internationalen Unternehmen schon wegen der komplexeren Geschäftsstrukturen oft notwendig, in diesen Fällen kann und sollte eine Datenschutzerklärung die erforderliche Transparenz schaffen. Die im Entwurf vorgeschlagene Einwilligung durch Opt-In und die weitergehenden Voraussetzungen hat jedoch zur Zielsetzung, dem unrechtmäßigen und übermäßigen Adresshandel entgegenzuwirken, wovon sich eine Datenverarbeitung im Konzern deutlich unterscheidet. Die besondere Warnfunktion, die durch Abs. 3a offenbar gewollt ist, muss sich von ihrem Sinn und Zweck her auf die Fälle beschränken, in denen Daten an Dritte weitergegeben werden, die der verantwortlichen Stelle in keiner Weise verbunden sind. Die Anwendung des § 3a in Unternehmensverbänden hingegen würden den Verbraucher eher verwirren und abschrecken.

2.6 Koppelungsverbot durch § 28 Abs. 3b BDSG

Das Koppelungsverbot ist in seiner Formulierung aus Sicht des BITKOM missglückt. Ausweislich der Begründung soll es nur bei Unternehmen mit marktbeherrschender Stellung greifen. Der Gesetzesformulierung lässt sich dies aber nicht entnehmen. In der Gesetzesanwendung soll das Tatbestandsmerkmal der marktbeherrschenden Stellung durch die Beschränkung konstruiert werden,

Stellungnahme

Änderung BDSG und Regelung Datenschutzaudit

Seite 8

dass es nur greift, „wenn dem Betroffenen ein anderer Zugang zu der vertraglichen Gegenleistung ... nicht... möglich ist“. Die Formulierung „vertragliche Gegenleistung“ ist aber unglücklich, weil sich diese Formulierung auf die spezifisch aus dem Vertrag mit dem jeweiligen Unternehmen geschuldete Leistung zu beziehen scheint. Dann wäre aber jedes Unternehmen von Absatz 3b unmittelbar betroffen, was nicht Sinn und Zweck sein kann. Grundsätzlich sollte eine solche Regelung sich daher unmittelbar und direkt an die Vorbilder in TMG und TKG anlehnen. Dort ist von „diesen TK-Diensten“ bzw. „diesen Telemedien“ die Rede, wodurch zum Ausdruck kommt, dass es eben nicht um Zugang zu dem Angebot eines speziellen Unternehmens, sondern um den Zugang zu vergleichbaren Angeboten anderer Unternehmen geht. Insofern sollte nach Ansicht des BITKOM formuliert werden: „wenn dem Betroffenen ein anderer Zugang zu vergleichbaren Leistungen anderweitig ohne die Einwilligung nicht oder in nicht zumutbarer Weise möglich ist“.

3 Stärkung des betrieblichen Datenschutzbeauftragten, § 4f Abs. 3 Satz 5e

Die Stärkung des betrieblichen Datenschutzbeauftragten durch Fort- und Weiterbildung ist ein unterstützenswerter Ansatz, den wir begrüßen. Aus Sicht des BITKOM ist die Sicherung der inhaltlichen Qualifikation aber nur eine der notwendigen Maßnahmen. Über die fachliche Qualifikation hinaus sollte auch seine Stellung im Unternehmen in einer Weise gefestigt und abgesichert werden, die zum einen den anderen betrieblichen Beauftragten vergleichbar ist, zum anderen aber vor allem ein Agieren ohne Scheu vor Konflikten ermöglicht. Das könnte durch einen erweiterten und spezifischen Kündigungsschutz erreicht werden, der während und nach der Tätigkeit als betrieblicher Datenschutzbeauftragter greift.

4 § 44 a BDSG, Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

Eine Benachrichtigungspflicht wird zukünftig für den Bereich der Telekommunikation durch novellierte europäische Vorgaben Eingang in das deutsche Recht finden. Nach Ansicht des BITKOM ist es jedoch fraglich, ob eine Ausweitung dieser Verpflichtung auf alle Unternehmen sinnvoll und erforderlich ist. Das in der Entwurfsbegründung zitierte Beispiel USA ist auf Deutschland nicht übertragbar, da in den USA eine andere Datenschutzgesetzgebung existiert und insbesondere kein betrieblicher Datenschutzbeauftragter in den Unternehmen zu bestellen ist. Der betriebliche Datenschutzbeauftragte muss aber schon aufgrund der jetzigen Bestimmungen des BDSG (§ 33 Abs. 1 S. 3) prüfen, ob von einer Unregelmäßigkeit betroffene Personen zu informieren sind (dies ergibt sich auch aus der allgemeinen Schadensminderungspflicht). Die Festschreibung einer Informationspflicht würde gegenüber der heutigen Pflicht zur Abwägung eine Verschlechterung darstellen. Bezweifelt werden muss auch der Nutzen der Information für den Betroffenen. Wenn jedoch eine allgemeine Informationspflicht eingeführt wird, ist uns nicht nachvollziehbar, warum öffentliche Stellen davon ausgenommen werden sollen. Das Bedürfnis des Betroffenen nach Information ist in Fällen von „Datenlecks“ bei öffentlichen Stellen in gleicher Weise zu bejahen wie bei Regelwidrigkeiten in Unternehmen.

Stellungnahme

Änderung BDSG und Regelung Datenschutzaudit

Seite 9

Über die Frage der Erforderlichkeit hinaus ist die Formulierung im Entwurf durch viele unbestimmte Rechtsbegriffe aus Sicht des BITKOM sehr problematisch. Konkretisiert werden müssten insbesondere die Nummern 3 und 4 der Aufzählung potentiell betroffener Daten. Zudem ist klarzustellen, dass verschlüsselte Daten in keinem Fall der Benachrichtigungspflicht nach § 44a BDSG unterliegen. Das stellen im Übrigen auch alle 46 US-Staaten mit entsprechender Gesetzgebung heraus.

Unklar ist darüber hinaus, was der „Verfügungsbereich“ ist und welche Konstellationen unter die Formulierung „auf sonstige Weise zur Kenntnis gelangt“ fallen. Und so begrüßenswert die Einführung einer Erheblichkeitsschwelle ist, so schwammig bleiben die Formulierungen. Der Entwurf legt fest, dass „schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdige Interessen des Betroffenen“ drohen müssen. Insoweit sind Konkretisierungen erforderlich, zum Beispiel dahingehend, dass lediglich schwerwiegende Datenschutzverstöße, die erhebliche wirtschaftliche Schäden oder soziale Nachteile einschließlich des Identitätsbetrugs zur Folge haben, die Benachrichtigungspflicht des Unternehmens auslösen.

Die Benachrichtigungspflicht sollte zunächst nur zum Inhalt haben, dass die zuständige Aufsichtsbehörde zu informieren ist, mit der dann das weitere Vorgehen und die Frage der Benachrichtigung der Betroffenen gemeinsam geklärt werden kann. Dabei müsste sichergestellt werden, dass keine unterschiedlichen Einschätzungen seitens der Aufsichtsbehörden vorgenommen werden.

Die den Unternehmen gegebene Alternative zur Information durch Anzeigen stellt z.B. in allen Fällen, in denen die Anzahl der Betroffenen gering ist, diese aber nicht ermittelt werden können, für das Unternehmen eine unverhältnismäßige Belastung dar. Die Unverhältnismäßigkeit der Belastung ergibt sich dabei zum einen aus den Kosten, die dem Unternehmen aus der Schaltung einer Anzeige entstehen, zum anderen aber auch aus der Schädigung des Ansehens des Unternehmens.

5 § 47, Übergangsregelung

Aus Sicht des BITKOM ist wegen der erheblichen und umfassenden notwendigen Umstellungen in den Unternehmen eine Übergangsfrist von drei Jahren unumgänglich. Die Altbestände an Daten müssten mindestens ebenso lange von den Unternehmen genutzt werden können.

6 Datenschutzauditgesetz

Hinweisen müssen wir zunächst darauf, dass eine umfassende und vollständige Einschätzung der zukünftigen Situation anhand des vorliegenden Entwurfs nicht möglich ist, da zum einen die zur Verfügung stehende Zeit für eine eingehende Analyse der Vorschriften nicht annähernd reicht und zum anderen wichtige Teilbereiche (insbesondere Form und Verfahren der Beleihung der Kontrollstellen sowie deren Mitwirkung, die Einzelheiten der Verwendung des Datenschutzauditsiegels und die Ausgestaltung der Kontrollverfahren sowie die Ein-

Stellungnahme

Änderung BDSG und Regelung Datenschutzaudit

Seite 10

zelheiten der Antragstellung) gemäß § 16 der späteren Regelung durch Rechtsverordnungen überlassen bleiben.

Im Gesetzentwurf enthaltene Redaktionsfehler zeigen deutlich, dass bei der Entwurfsverfassung nicht die angemessene Sorgfalt angewendet werden konnte. Unbedingt sinnvoll wäre daher eine Verlängerung des Erörterungsverfahrens um wenigstens vier Wochen.

Die folgenden Ausführungen stehen daher insgesamt unter dem Vorbehalt der späteren Ergänzung und Vertiefung.

6.1 Bedarf und Nutzen

BITKOM steht der Regelung eines Datenschutzauditgesetzes grundsätzlich aufgeschlossen gegenüber. Das Ziel der Regelungen zum Datenschutzaudit kann aus Sicht des BITKOM jedoch nur sein, ein schlankes, begrenztes, praxisorientiertes und für die Unternehmen akzeptables Verfahren einzuführen.

Ausgangspunkt des Gesetzgebungsvorhabens zu einem Bundesdatenschutzaudit-Gesetz ist § 9a BDSG, der die gesetzliche Regelung eines Audits ermöglicht:

„Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt.“

Das Anliegen des Gesetzgebers bei der Aufnahme des § 9a BDSG war es, die Intentionen und Vorgaben des BDSG dadurch zu verstärken, dass datenverarbeitende Stellen und Anbieter ihre Verfahren bzw. Produkte freiwillig in einem externen Qualitätsprüfungsprogramm begutachten lassen. Bei erfolgreicher Auditierung soll ein Zusatznutzen erreicht werden, insbesondere ein positives Image des Unternehmens, Stärkung des Vertrauens und Marktvorteile. Zugleich soll (so auch die Begründung des vorliegenden Referentenentwurfs) dem Verbraucher die Möglichkeit einer Marktorientierung bezüglich datenschutzgerechter Produkte bzw. Dienstleistungen gegeben werden.

Ungeachtet des Umstands, dass die Möglichkeit eines Datenschutzaudits und seine gesetzliche Regelung im BDSG angelegt sind, ist nach Auffassung des BITKOM ein Nutzen für die Unternehmen alles andere als selbstverständlich. Eine Eignung als Differenzierungskriterium im Wettbewerb sehen unsere Mitgliedsunternehmen nur punktuell. Sollen die Unternehmen der ITK-Branche gleichwohl in möglichst großem Umfang von der Möglichkeit der Auditierung Gebrauch machen, muss der Nutzen eines Datenschutzaudits über einen abstrakten Wettbewerbsvorteil hinaus gezielt als Teil des Datenschutzauditgesetzes regulativ ermöglicht und gesichert werden.

Aufgrund der aufgezeigten Problemkreise und unserer Erfahrungswerte (zum Beispiel mit ISO-Zertifizierungen) erscheint es uns sehr fraglich, ob sich die Einführung eines Gütesiegel allein mit dem Hinweis auf einen möglichen Wett-

Stellungnahme

Änderung BDSG und Regelung Datenschutzaudit

Seite 11

bewerbsvorteil für die Unternehmen etablieren lassen wird. Ein greifbarer Nutzen für die Unternehmen könnte jedoch in der Weise erreicht werden, dass die Auditierung für das Unternehmen mit unmittelbaren Erleichterungen oder Entlastungen bei der datenschutzrechtlichen Einbettung gekoppelt ist. Beispiele hierfür sind:

- der konzerninterne Datentransfer,
- der Datentransfer in nicht sichere Drittstaaten,
- die Anerkennung der Auswahl auditierten Dienstleister und Verfahren als Erfüllung der Sorgfaltspflicht im Rahmen der Auftragsdatenverarbeitung nach § 11 Abs. 2 BDSG durch die Aufsichtsbehörden,
- die telefonische Einholung von Einwilligungen,
- die Nutzung des Listenprivilegs, das durch die Änderungen im BDSG gestrichen werden soll,
- der Verzicht auf Zufallskontrollen durch Datenschutzaufsichtsbehörden und
- Haftungsprivilegierungen.

Eine vergleichbare Haftungsprivilegierung ist im Jugendschutzrecht mit dem neuen Jugendmedienschutzstaatsvertrag in § 20 Abs. 5 JMStV erstmals eingeführt worden. Danach dürfen die Jugendschutzaufsichtsbehörden Produkte, die bereits von den Prüfern der anerkannt freiwilligen Selbstkontrolle geprüft sind nur noch überprüfen, soweit die Prüfer dabei die Regeln des Beurteilungsspielraumes überschritten haben oder aber wenn ein entsprechender Anlass gegeben ist, etwa ein sehr schwerwiegender Verstoß gegen das Jugendschutzrecht. Dieses sehr erfolgreiche Modell aus dem Jugendschutzrecht kann und sollte auch auf das Datenschutzrecht übertragen werden. Auf diese Weise könnte dem Datenschutzgütesiegel und den zertifizierten Unternehmen ein echter Mehrwert geboten werden. Im Bereich der Unternehmenskonzepte kann über diese Systematik die Rechtskonformität eines Unternehmens z.B. für einen bestimmten Zeitraum vermutet werden, wenn nicht ein Anlass erheblichen Grund zum Zweifel gibt oder der Verdacht besteht, dass die Prüfung nicht ordnungsgemäß erfolgt ist.

Nicht nachvollziehbar ist uns, warum die öffentlichen Stellen von der Möglichkeit der Auditierung ausgenommen werden. Unabhängig vom Bestehen eines Wettbewerbsvorteils und ungeachtet der Frage, ob der Bürger sich an eine andere Behörde wenden kann, wird ihn regelmäßig (und nicht anders als gegenüber Unternehmen) die Frage interessieren, ob die verarbeitende Stelle mit seinen Daten rechtskonform umgeht. Die mögliche Gefährdung des Bürgers durch rechtswidrige Datenverarbeitung ist ebenfalls nicht abweichend zu beurteilen. Insoweit wird also in willkürlicher Weise mit zweierlei Maß gemessen. Im Übrigen wäre ja auch für die öffentlichen Stellen ein Audit freiwillig so dass sich also kein Zwang ergäbe, während mit der jetzigen Regelung den öffentlichen Stellen die Möglichkeit zur Auditierung grundlos verbaut wird.

6.2 § 1, Maßstab und Gegenstand des Datenschutzaudits

6.2.1 Auditgegenstand

Gegenstände des Audits können gemäß § 1 Abs. 1 des Entwurfs ein Datenschutzkonzept sowie technische Einrichtungen der beantragenden Stelle sein.

Stellungnahme

Änderung BDSG und Regelung Datenschutzaudit

Seite 12

Durch diese Terminologie wird das DSAG unmittelbar mit § 9a BDSG verzahnt. Diese Lösung ist nach Ansicht des BITKOM fragwürdig. Weder das BDSG noch das DSAG geben eine Legaldefinition des „Datenschutzkonzepts“ und der „technischen Einrichtung“, so dass unklar bleibt, ob auch Verfahren und Produkte mögliche Auditgegenstände sein können, da sich dies nicht ohne Weiteres aus den Begriffen „Datenschutzkonzept“ und „technische Einrichtung“ ergibt.

Wir regen daher an, Absatz 1 offen und ohne Erwähnung bestimmter Antragsgegenstände zu formulieren, z.B.

„Anbieter von Datenverarbeitungssystemen und -programmen und verantwortliche Stellen können ein Datenschutzaudit nach Maßgabe dieses Gesetzes freiwillig durchführen. Den Gegenstand des Datenschutzaudits legt der Anbieter bzw. die verantwortliche Stelle fest.“

Aus Sicht der Wirtschaft ist es unerlässlich, dass der Gegenstand des Audits flexibel und individuell zu bestimmen ist. Nur so kann ein angemessenes Verhältnis von Aufwand und Nutzen sichergestellt und der unternehmensspezifischen Situation Rechnung getragen werden. Das Konzept, das § 1 des Entwurfs zugrunde liegt, findet deshalb unsere Unterstützung. Wir schlagen jedoch vor, nicht nur in der Begründung, sondern auch im Gesetz klarzustellen, dass der Umfang des Audits der Dispositionsfreiheit des Antragstellers unterliegt und daher z.B. auf Teile der Organisation oder einzelne Einrichtungen oder Produkte beschränkt sein kann.

6.2.2 Maßstab der Auditierung

Als Maßstab der Auditierung legt § 1 kumulativ vier Anforderungen fest:

- Erfüllung der gesetzlichen Anforderungen bzgl. des Auditgegenstandes,
- Erfüllung der (noch zu definierenden) Richtlinien zur Verbesserung des Datenschutzes (§ 11),
- Erfüllung der Vorschriften zur Stellung des betrieblichen Datenschutzbeauftragten,
- Teilnahme an regelmäßigen Kontrollen.

Diesen Maßstab halten wir insgesamt für sachgerecht. Er steht und fällt allerdings mit der Qualität der noch zu definierenden Richtlinien.

Die Richtlinien zur Verbesserung des Datenschutzes können ein sinnvolles Instrument sein, wenn sichergestellt wird, dass in großem Ausmaß unternehmensspezifische und sektor- bzw. branchenspezifische Anforderungen und Erfahrungen Berücksichtigung finden.

Durch § 11 Abs. 1 Satz 1 des Entwurfs wird klargestellt, dass Gegenstand der Richtlinien nicht nur der Datenschutz, sondern auch die Datensicherheit ist. Das ist aus Sicht des BITKOM sachgerecht, da im Entwurf ausdrücklich die technischen Einrichtungen als Gegenstand eines Audits erwähnt werden und durch § 9 BDSG Überschneidungen zwischen Datenschutz und Datensicherheit ohnehin angelegt sind. Auch in der Praxis würde die Abgrenzung des Datenschutzes von der Sicherheit informationstechnischer Systeme und Komponenten Schwierigkeiten bereiten. BITKOM regt insoweit an, dass eine Anrechnung bestehender Zertifizierungen (insbesondere für IT-Sicherheitsmanagement Systeme) vorgesehen wird.

Stellungnahme

Änderung BDSG und Regelung Datenschutzaudit

Seite 13

Unklar ist § 1 Nr. 4, der „regelmäßige“ Kontrollverfahren vorschreibt. Nicht ersichtlich ist, wie häufig ein Unternehmen kontrolliert wird, was ein Kontrollverfahren auslöst und wer die diesbezügliche Entscheidung trifft. Offen ist auch das Verhältnis zur Regelung in § 3 a. E., die eine Kontrolle mindestens einmal jährlich fordert. Dies muss in der gesetzlichen Regelung klargestellt werden, wobei die Entscheidung in die Hand der verantwortlichen Stelle gelegt werden muss.

6.2.3 Freiwilligkeit des Audits

Jedes Datenschutzaudit muss freiwillig sein. BITKOM begrüßt daher, dass der Entwurf in § 1 Abs. 1 die Freiwilligkeit zugrunde legt und zum Ausdruck bringt. In diesem Zusammenhang weisen wir auf unseren Formulierungsvorschlag oben 7.2.1 hin, der die Freiwilligkeit in den Gesetzestext aufnimmt.

Wichtig ist es uns, nachdrücklich darauf hinzuweisen, dass diese Freiwilligkeit keinesfalls durch die Einbeziehung der Zertifizierung als Kriterium bei der Vergabe von Aufträgen durch die öffentliche Hand faktisch unterlaufen werden darf. Eine derartige Verbindung des Datenschutzgütesiegels mit der öffentlichen Auftragsvergabe würde die Freiwilligkeit einer Prüfung für die überwiegende Anzahl der Unternehmen illusorisch machen. Letztlich läge darin ein massiver faktischer Eingriff in den Wettbewerb.

6.3 Verfahren der Auditierung, §§ 1 - 6

Das Ziel der Regelungen zum Datenschutzaudit kann aus Sicht des BITKOM nur sein, ein schlankes, begrenztes, praxisorientiertes und für die Unternehmen akzeptables Verfahren einzuführen. Das mit dem Entwurf gewählte einstufige Verfahren ist dem zweistufigen Modell daher uneingeschränkt vorzuziehen. Für die Ausgestaltung als einstufiges Verfahren sprechen auch die bisherigen Erfahrungen mit der Zertifizierung von Qualitäts-, Umwelt-, Sicherheitsmanagementsystemen (ISO 9001, 140001, 270001), bei denen es sich um von der Industrie anerkannte, seit langem praktizierte einstufige Verfahren handelt.

Nach Auffassung des BITKOM ist zudem von zentraler Wichtigkeit, dass es bei dem gesamten Verfahren zu keinerlei unterschiedlichen Anforderungen und Rechtsfolgen kommt. Wenn Datenschutz durch ein Gütesiegel ausgewiesen werden soll, dann kann ein solches Gütesiegel nur ein einheitliches und bundesweit greifendes Gütesiegel sein. Regionale, lokale oder sektorale Einzellösungen sind für die Wirtschaft inakzeptabel.

Länderübergreifender Wirtschaftstätigkeit dürfen keine störenden Schranken entgegengesetzt werden. Zu begrüßen ist daher die Möglichkeit für Kontrollstellen, bundesweit tätig zu sein. Für Unternehmen, die in unterschiedlichen Bundesländern aktiv sind, schafft das die erforderliche Flexibilität. In diesen Konstellationen muss es möglich sein, dass die Unternehmen unabhängig vom Sitz der jeweiligen Niederlassung die gleiche Kontrollstelle beauftragen. Wichtig ist dies, um die Auditierungen effizient durchführen zu können, Kosten zu sparen und die Einheitlichkeit der Zertifikate sicherzustellen.

Stellungnahme

Änderung BDSG und Regelung Datenschutzaudit

Seite 14

Wir begrüßen daher grundsätzlich die entsprechenden Regelungen in den §§ 1 - 6 des Entwurfs und die diesbezüglichen Passagen in der Entwurfsbegründung mit Ausnahme des § 5 Abs. 3.

6.4 Dauer der Berechtigung, das Datenschutzauditsiegel zu verwenden

Der Entwurf bindet die Berechtigung eines Unternehmens, das Datenschutzauditsiegel zu verwenden, in zeitlicher Hinsicht an die regelmäßige Überprüfung durch die Kontrollstellen. Diese Regelungstechnik erscheint aus Sicht der ITK-Branche sachgerecht, da sie der für die ITK-Branche prägenden raschen Abfolge unterschiedlicher Produkt- und Verfahrenszyklen bzw. Verbesserungen, bei denen erfahrungsgemäß der Lebenszyklus unveränderter Produkte in Monaten gemessen wird, nicht entgegensteht. Das im Entwurf gewählte Verfahren könnte bei den Unternehmen die Akzeptanz und Attraktivität einer Auditierung durchaus fördern; zudem würde der Verwaltungsaufwand bei der Führung des Verzeichnisses (§ 8) gering gehalten.

Eine Regelung, die für die Auszeichnung eines bestimmten Auditgegenstand mit dem Siegel einen festgelegten Gültigkeitszeitraum festlegt, würde an dieser Wirklichkeit vollständig vorbei gehen. Sie hätte zur Folge, dass das Datenschutzauditsiegel nur für das Produkt (Technische Einrichtung) oder nur für das Konzept gültig ist, das der Kontrollstelle baugleich oder textidentisch als Prüfmuster vorgelegen hat. Würde das Produkt bzw. das Konzept gegenüber dem evaluierten Prüfmuster verändert, müsste das Verfahren erneut durchgeführt werden. Das würde letztlich dazu führen, dass ein Produkt, für das das Verfahren noch nicht abgeschlossen ist, schon zugunsten seines Nachfolgers vom Markt genommen würde. Eine derartige Regelung dürfte in den Unternehmen häufig zu einer Entscheidung gegen eine Zertifizierung führen, da das Verfahren unattraktiv und unpraktikabel ist.

Stellungnahme

Änderung BDSG und Regelung Datenschutzaudit

Seite 15

6.5 Zuständigkeit, § 2

Aus Abs. 1 Satz 2 könnte für manche Unternehmen – je nach betroffener Datenverarbeitung – eine Doppelzuständigkeit (Bund / Land) resultieren. Ein Nebeneinander zweier Zuständigkeiten sollte aber auf jeden Fall vermieden werden. Je nach Schwerpunkt der Datenverarbeitung durch das Unternehmen sollte im Einvernehmen von Land und Bund eine einzige Zuständigkeit begründet werden.

6.6 § 3 Satz 2, Einbeziehung des betrieblichen Datenschutzbeauftragten

BITKOM begrüßt die ausdrückliche Einbeziehung des betrieblichen Datenschutzbeauftragten in die Durchführungen der Kontrollen. Ein Datenschutzaudit darf nicht zu einer Schwächung der Position betrieblicher Datenschutzbeauftragter führen, sondern vielmehr zu deren Stärkung, so dass deren aktive Einbindung in den Zertifizierungsprozess sichergestellt sein sollte. Hierdurch kann der Eindruck vermieden werden, dass die Funktion des betrieblichen Datenschutzbeauftragten überprüft wird.

Die konkrete Formulierung des § 3 erscheint uns jedoch problematisch. So ist zunächst unklar, warum Satz 1 eingeleitet wird durch „*Vorbehaltlich einer Rechtsverordnung...*“. Systematisch wäre dies als Einschränkung zu verstehen, für die wir jedoch keinen Raum und Anlass sehen.

Zudem ist die Formulierung der Einbeziehung des betrieblichen Datenschutzbeauftragten zu offen. Erforderlich ist eine klare Abgrenzung der Aufgaben der Kontrollstelle und der Tätigkeit des betrieblichen Datenschutzbeauftragten, die wir vor allem in der Vorbereitung und Unterstützung sehen. Insbesondere ist Aufgabe des Beauftragten nicht die Mängelbeseitigung (so aber die Begründung zum Entwurf), denn dafür ist die jeweilige Fachstelle im Unternehmen zuständig.

Wir schlagen daher vor, dass die Rolle und die Aufgaben des betrieblichen Datenschutzbeauftragten bei der Durchführung der Kontrollen durch den Ausschuss nach § 11 DSAG konkretisiert wird.

6.7 § 4, Zulassung der Kontrollstellen und Entziehung der Zulassung

§ 4 Abs. 3 des Entwurfs ist aus Sicht des BITKOM bedenklich weit und unbestimmt gefasst. Die Möglichkeit, sich für Einschränkungen der Zulassung der Kontrollstellen auf „Belange des Datenschutzes“ zu berufen, gibt den Kontrollstellen nicht die erforderliche Transparenz, Orientierung und Rechtssicherheit.

6.8 § 5, Pflichten der Kontrollstelle, Kontrahierungszwang

Nach unserer Einschätzung ist für einen Kontrahierungszwang als weitgehenden Eingriff in die Privatautonomie kein Bedarf ersichtlich. Falls sich wegen des Verhältnisses von Angebot und Nachfrage später zeigen sollte, dass die Berücksichtigung aller interessierten Unternehmen zum Funktionieren des Systems

Stellungnahme

Änderung BDSG und Regelung Datenschutzaudit

Seite 16

sichergestellt werden muss, könnte der Kontrahierungszwang auch dann noch eingefügt werden.

In Absatz 2 Satz 1 wird festgelegt, dass für Ausnahmen vom Kontrahierungszwang die zuständige Landesbehörde und der Bundesbeauftragte zuständig sind. Dieses Nebeneinander von Bund und Land ist weder systematisch noch inhaltlich nachvollziehbar. Sollte die Zuständigkeit nicht kumulativ, sondern alternativ gemeint sein, wäre die Abgrenzung unklar. Nach Einschätzung des BITKOM läge es in der Konsequenz von § 2 Abs. 2 des Entwurfs, dass die Ausnahmen vom Kontrahierungszwang ebenfalls (nur) vom Bundesbeauftragten zugelassen werden.

Nach Absatz 2 von § 5 übermittelt die Kontrollstelle den zuständigen Behörden ein Verzeichnis der „nicht öffentlichen Stellen“, die ihrer Kontrolle unterstanden. Im Zusammenspiel mit § 1 S. 1 ergeben sich sprachliche und systematische Unklarheiten. Die in § 1 S. 1 erfassten „Anbieter von Datenverarbeitungssystemen und -programmen“ wären von § 5 Abs. 2 nur erfasst, wenn man in § 1 S. 1 die „nicht öffentlichen Stellen“ als Oberbegriff sowohl für die Anbieter von Datenverarbeitungssystemen und -programmen als auch für die zusätzlich erwähnten „verantwortlichen Stellen“ versteht. Dieses Verständnis ergibt sich aus § 1 S. 1 jedoch nicht zweifelsfrei. Die gleiche Problematik stellt sich im Zusammenhang mit Abs. 4 des § 5.

Die unverzügliche Unterrichtungspflicht in Abs. 3 S. 2 ist aus Sicht des BITKOM hoch problematisch. Diese Regelung könnte zu erheblichen Akzeptanzproblemen auf Seiten der grundsätzlich an einem Audit interessierten Unternehmen führen. Denn faktisch würde sie zu einer Schlechterstellung gegenüber den nicht auditierungswilligen Unternehmen führen. Zudem könnte die Regelung eine Störung des Vertrauensverhältnisses zur Kontrollstelle zur Folge haben. Ziel muss es sein, den Kontrollstellen ein den Wirtschaftsprüfern vergleichbares Handeln zu ermöglichen. Wir schlagen daher vor eine Regelung zu formulieren, die es der Kontrollstelle ermöglicht, zunächst intern Abhilfe vom zu auditierenden Unternehmen zu fordern und bis dahin die Freigabe zurückzustellen. Auf diese Weise kann sichergestellt werden, dass die Verantwortlichkeit zunächst im Rahmen des Kontrollverfahrens bleibt. Erst dann, wenn einem Verstoß nicht abgeholfen wird, sollte die Aufsichtsbehörde unterrichtet werden. Die Unterrichtungspflicht der Kontrollstelle sollte dabei auch nach erfolglosem Ablauf einer Abhilfefrist nicht bei jedem, evtl. unbedeutenden Verstoß bestehen, sondern sie sollte einer Erheblichkeitsschwelle unterliegen. Für die Aufsichtsbehörde hat dies zudem den Vorteil, dass sie sich auf die wirklich wichtigen Fälle konzentrieren kann.

6.9 § 6, Überwachung der Kontrollstellen durch die zuständigen Behörden

Abs. 1 Satz 1 regelt, dass eine Kontrollstelle von der zuständigen Behörde des Landes, in dem die Kontrollstelle ihre jeweilige Tätigkeit ausübt, überwacht wird. Diese „dynamische Zuständigkeit“ ist nach Einschätzung des BITKOM für keinen der Beteiligten sinnvoll. Wir plädieren daher dafür, die Überwachung auf die Aufsichtsbehörde zu beschränken, in deren Zuständigkeitsbereich die Kontrollstelle ihre Niederlassung hat.

Stellungnahme

Änderung BDSG und Regelung Datenschutzaudit

Seite 17

Ebenso wenig nachvollziehbar ist die Regelung in Absatz 2, nach der die Dauer einer Untersagung bezüglich der Kennzeichnung mit dem Siegel der Vereinbarung mit der zuständigen Behörde unterliegt. Hier läge es wesentlich näher, dass die Dauer der Untersagung an die Behebung des fraglichen Verstoßes gekoppelt wird.

6.10 § 8, Kennzeichnung mit dem Datenschutzauditsiegel, Verzeichnisse

Die Möglichkeit, im Internet einsehbar zu machen, wer ein Datenschutzauditsiegel verwendet und auf was sich dieses bezieht, halten wir grundsätzlich für eine sachgerechte Lösung, die die notwendige Transparenz und Orientierung für alle Marktteilnehmer sicherstellt.

Unklarheiten sehen wir jedoch in Einzelheiten der Formulierung des Absatzes 2 Satz 2, denn es ist nicht klar ersichtlich, was letztlich alles ins Verzeichnis kommt. Möglicherweise müsste in der Nr. 1 ein „sowie“ eingefügt werden, um den Regelungsgehalt klarzustellen.

Fraglich erscheint aber ohnehin, welcher Mehrwert an Information durch die Angabe der alphanumerischen Identifikationsnummer im Zusammenhang des Absatzes 2 erreicht wird, da es dafür kein Verzeichnis gibt.

6.11 § 9, Anforderungen an Kontrollstellen

Die systematische Trennung der Bereiche „Recht“ und „Informationstechnik“ in Absatz 3 des § 9 ist im Gesamtzusammenhang des Entwurfs ein systematischer Fremdkörper, er findet sich an keiner anderen Stelle im Gesetz. Wir halten diese Trennung daher für entbehrlich. Es fehlt darüber hinaus auch die Klarstellung, wie sich die einzelnen Ziffern zu einander verhalten – gemeint ist offenbar eine Alternative, weil die jeweilige Kumulierung der dreijährigen beruflichen Tätigkeit mit der fünfjährigen beruflichen Tätigkeit unsinnig wären. Insoweit ist wohl eine Klarstellung durch die Einfügung eines „oder“ erforderlich.

6.12 § 12, Mitglieder des Datenschutzauditausschusses, Berufung und Vorschlagsrecht

Ein Zweidrittel-Übergewicht der Vertreter aus dem öffentlichen Bereich ist aus Sicht des BITKOM nicht zielführend. Wir schlagen vor, die Zahl der Unternehmen auf acht zu erhöhen. Im Interesse der Akzeptanz und Nutzung der Auditierungsmöglichkeit ist es unerlässlich, in breitem Maß unternehmensspezifische und sektor- bzw. branchenspezifische Anforderungen und Erfahrungen in die Richtlinien einzubringen und sicherzustellen, dass alle wesentlichen Gruppen hinter den Richtlinien stehen. Da die Erfahrung aus der Perspektive der Aufsicht auch durch die Vertreter des Bundesbeauftragten eingebracht wird, kann die Anzahl der Vertreter der Länderaufsichtsbehörden auf zwei reduziert werden.

Stellungnahme

Änderung BDSG und Regelung Datenschutzaudit

Seite 18

6.13 § 17 Bußgeldvorschrift

Da BITKOM die Unterrichtungspflicht des § 5 Abs. 3 in der vorgeschlagenen Form ablehnt, wenden wir uns auch gegen die entsprechenden Bußgeldandrohungen als Teil eines freiwilligen Verfahrens.

Die Verhängung eines Bußgeldes bei mangelnder Kooperation bei einem freiwilligen Audit, wie in Nr. 5 und 6 vorgesehen, ist unangemessen. Die Sanktion sollte vielmehr in einem Abbruch des Auditverfahrens und einer Verweigerung des Siegels bestehen, möglicherweise verbunden mit einer Karenzzeit für die Neubeantragung des Siegels.

6.14 § 18, Strafvorschrift

BITKOM hält die Strafvorschriften zum Teil für zu weitgehend. Der Vergleich mit den Wertungen des § 43 BDSG zeigt, dass eine weitergehende Differenzierung erforderlich ist. Schwierigkeiten dürfte auch das Merkmal der Bereicherungsabsicht bereiten. Denn wenn die Verwendung des Datenschutzauditsiegels eine Marktrelevanz hat, wie es die Begründung des DSAG an vielen Stellen ausdrücklich und implizit voraussetzt, dann dürfte ein Handeln in Bereicherungsabsicht immer vorliegen, wenn das Siegel verwendet wird. Eine unterscheidende oder qualifizierende Funktion kommt dem Merkmal dann aber nicht mehr zu.

6.15 § 19, Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

BITKOM begrüßt nachdrücklich, dass durch § 19 DSAG an die erfolgreiche Auditierung eine unmittelbare Privilegierung für das auditierte Unternehmen gebunden wird. Diese Vorschrift sollte durch weitere Vorschriften zu Erleichterungen bei der datenschutzrechtlichen Einbettung ergänzt werden, z.B. durch die Erlaubnis zur Nutzung des Listenprivilegs u.a. (vgl. dazu schon oben 2.3 und 7.1).

Nach unserem Verständnis ist Satz 1 des § 19 DSAG aber sprachlich misslungen. Nicht klar wird, ob die Ziffern 1 bis 6 als Einschränkung oder Präzisierung gemeint sind. Unklar ist auch das Verhältnis zu § 44a BDSG. Aus Sicht der Unternehmen ist es insbesondere unbefriedigend, dass nicht deutlich wird, welche weiteren Schritte sich (aus anderen Vorschriften des DSAG oder BDSG) an die Unterrichtung der Kontrollstelle anschließen können.

6.16 Sonstiges

Nicht nur dort, wo Produkte oder Systeme vom Nutzer individuell konfiguriert werden können, hat der Hersteller wenig Einfluss auf die Art und Weise des tatsächlichen Produkt- bzw. Systemeinsatzes. Es muss daher die Frage aufgeworfen werden, ob es wirklich sinnvoll ist, die Verantwortlichkeit für den Datenschutz umfassend in die Sphäre des Herstellers zu verlagern. Denn der Hersteller kann höchstens die Voraussetzungen für einen datenschutzgerechten Einsatz schaffen, die Erfüllung dieser Voraussetzungen und datenschutzrechtlichen

Stellungnahme

Änderung BDSG und Regelung Datenschutzaudit

Seite 19

Anforderungen liegt letztlich jedoch allein in der Hand des jeweiligen Anwenders. Der Nutzer muss daher für einen datenschutzgerechten Einsatz von Produkten sensibilisiert und zu einem verantwortungsbewussten Umgang befähigt werden.

Ähnlich liegt das Problem in den häufigen Konstellationen, dass das Produkt oder System nicht isoliert, sondern als eine von vielen Komponenten eines Gesamtsystems zum Einsatz kommt. Auch hier ist das Zusammenspiel der Komponenten und dessen datenschutzrechtliche Konformität dem Einfluss des einzelnen Herstellers entzogen.

Schließlich berücksichtigt der Entwurf nicht, dass heute die internationale Verarbeitung von Daten häufig der Regelfall ist. So wird zum Beispiel keine Aussage getroffen, ob ein Subunternehmer ebenfalls das Auditsiegel besitzen muss, bevor der Auftraggeber dieses bekommen kann – die Einschaltung von Subunternehmern / Auftragnehmern ist heute aber in vielen Fällen Standard. Eine weitere offene Frage: Wie verhält es sich mit Subunternehmern im / aus dem Ausland?