Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
16(4)561 E

BITKOM e.V. · Albrechtstraße 10 A · 10117 Berlin-Mitte

Berlin, 13. März 2009

Kabinettsentwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes und zur Regelung des Datenschutzaudits

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

Sehr geehrte Damen und Herren,

in den kommenden Wochen wird im Bundestag und seinen Ausschüssen der Kabinettsentwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes und zur Regelung des Datenschutzaudits beraten. Der Auslöser für diese gesetzgeberische Aktivität waren mehrere Fälle von eklatanten Datenschutzverstößen in der Wirtschaft, die –sehr nachvollziehbar – zu einer erheblichen Verunsicherung der Bürger geführt haben.

1. Sachgerechter Interessenausgleich

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. Es ist weder nachvollziehbar noch vermittelbar, dass in der aktuellen gesamtwirtschaftlichen Krise von der Bundesregierung milliardenschwere Konjunkturpakete geschnürt werden, während gleichzeitig Gesetze initiiert werden, die den Unternehmen den Weg zu ihren Kunden versperren.

Allen Vorfällen der letzten Monate ist gemeinsam, dass sie nicht im rechtsfreien Raum stattgefunden haben, sondern dass 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, sondern um den einseitigen Ausbau des Verbraucherschutzes. Wir befürchten, dass durch die Vorschläge keinesfalls das nötige Gleichgewicht zwischen den Interessen von Kunden und Unternehmen hergestellt wird, sondern vielmehr über das legitime Ziel der Missbrauchsbekämpfung hinaus bestimmte Werbeformen existentiell und sachwidrig eingeschränkt werden.

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

Vor diesem Hintergrund setzten wir uns für den Erhalt des Listenprivilegs ein. Maßstab ist für uns die gesetzgeberische Zielsetzung, vorsätzlichen Missbrauch von Daten zu verhindern und dadurch die Verbraucher zu schützen.

Ergänzt haben wir unsere Einschätzung mit zwei Beispielen aus der Praxis zum Direktmarketing und zum Adresshandel (vgl. Anlage 2). Wir glauben, dass diese Beispiele hilfreich sein können, um die realen und regelmäßigen Abläufe in diesen Bereichen und ihre Bedeutung für viele Unternehmen adäquat nachvollziehen zu können.

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

Der Gesetzentwurf 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 in unserer Stellungnahme unter Punkt 3.4 und 3.5 formuliert).

Seriöses Adressgeschäft ist für die deutsche Wirtschaft unverzichtbar. Laut dem aktuellen Direktmarketing-Monitor der Deutschen Post haben die Unternehmen in Deutschland im Jahr 2007 ca. 72 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 zehntausende Arbeitsplätze; es ist somit ein wichtiger Pfeiler unserer Volkswirtschaft. Gerade in der aktuellen, durch eine elementare Schwächung und Krise der Konjunktur geprägten Wirtschaftslage in Deutschland geht die Streichung des Listenprivilegs daher in eine völlig falsche Richtung.

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 – zehntausende Arbeitsplätze wären gefährdet. Gerade in der aktuellen, durch eine elementare Schwächung und Krise der Konjunktur geprägten Wirtschaftslage in Deutschland geht die Streichung des Listenprivilegs daher in eine völlig falsche Richtung.

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.

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.

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.

Aus Sicht der Wirtschaft muss ein erfolgreiches Audit mit unmittelbaren Erleichterungen und Entlastungen bei der datenschutzrechtlichen Einbettung des Unternehmens verbunden sein, 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 (Formulierungsvorschlag vgl. Stellungnahme 3.5). 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.

Der vorliegende Kabinettsentwurf regelt die Voraussetzungen für eine Datenschutzauditierung des Unternehmens. Vorgesehen ist, 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.

In der Diskussion um den vorliegenden Gesetzentwurf sind auch der Ausbau der sog. „Robinsonliste“, eine Stärkung des Widerspruchsrechts und die Kennzeichnung der Daten als weitere Lösungsansätze vorgeschlagen worden. Alle drei Vorschläge sind nach Einschätzung des BITKOM überlegenswerte Elemente, da sie –im Gegensatz zu dem Inhalt des vorliegenden Entwurfs- in unmittelbarer Weise mit den Zielen des Gesetzgebungsvorhabens verzahnt werden können. Möglich wäre das, in dem man diese Elemente als übergreifende Regelungen ausgestaltet, aber vor allem auch durch die Nutzung dieser Elemente als Teile einer Richtlinie, die der Maßstab für eine erfolgreiche Auditierung ist.

4. Position des BITKOM zum Kabinettsentwurf

In einer ausführlichen Stellungnahme haben wir unsere Kernforderungen und Positionen zu den Vorschlägen des Kabinettsentwurfs dargelegt. Die Stellungnahme finden Sie als Anlage 1 zu diesem Schreiben.

Mit freundlichen Grüßen,

Kai Kuhlmann

Anlagen

1. Ausführliche Stellungnahme des BITKOM zum Kabinettsentwurf (einschließlich der Kernforderungen)
2. Beispiel für Adress-/Datenhandel und Beispiel für Direktmarketing

ANLAGE 1

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

Inhalt

1 Kernforderungen

- **zum Bundesdatenschutzgesetz:**
  - Unternehmen, die gemäß dem künftigen Datenschutzauditgesetz auditiert worden sind, müssen weiterhin das Listenprivileg nutzen können (dazu unten 3.4). Eine entsprechende Regelung ist den Ausnahmen des § 28 Abs. 3 hinzuzufügen.
  - Eine Robinsonliste, die Stärkung des Widerspruchsrechts und eine Kennzeichnung der werblichen Ansprache, die die Rückverfolgbarkeit ermöglicht, können effektive Elemente einer Auditierungsrichtlinie sein.
  - Das Koppelungsverbot darf in keiner Weise über die Formulierung im TMG hinaus erweitert werden. Es muss ausdrücklich auf marktbeherrschende Unternehmen beschränkt sein; eine marktweite Betrachtung stellt eine gefährliche Erweiterung dar (dazu unten 3.6.2).
  - Die Übergangsvorschrift muss unmissverständlich regeln, dass die neuen Regelungen der §§ 28 und 29 erstmalig nach drei Jahren Anwendung finden. Einwilligungen, die gemäß § 4a BDSG wirksam abgegeben worden sind, müssen in ihrem bestand geschützt werden (dazu unten 7).
  - Die Anforderungen der Informationspflicht in § 42 a müssen den Unternehmen durch eindeutige und praxisgerechte Anforderungen Rechtssicherheit geben (dazu unten 6).

- **zum Datenschutzauditgesetz:**
  - Die Auditierung muss für das Unternehmen unmittelbare Erleichterungen oder Entlastungen bei der datenschutzrechtlichen Einbettung zur Folge haben (dazu unten 8.1).
  - Der Auditierungsgegenstand muss im Gesetz möglichst offen formuliert werden (dazu unten 8.2.1).
  - Die Pflicht der Kontrollstellen, die zuständige Aufsichtsbehörde über Verstöße zu unterrichten, muss umgestaltet werden: Vorrang der internen Abhilfe und Einfügung einer Erheblichkeitsschwelle (dazu unten 8.8).
  - Der Datenschutzauditausschuss, der die als Maßstab der Auditierung dienenden Richtlinien erlässt, muss paritätisch mit Vertretern von Unternehmern besetzt sein (dazu unten 8.12).

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 Kabinettsentwurfs zur Findung sachgerechter Regelungen beitragen zu können. Auch für den weiteren Dialog stehen wir gerne zur Verfügung.

2 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. Es ist weder nachvollziehbar noch vermittelbar, dass in der aktuellen gesamtwirtschaftlichen Krise von der Bundesregierung milliardenschwere Konjunkturpakete geschnürt werden, während gleichzeitig Gesetze initiiert werden, die den Unternehmen den Weg zu ihren Kunden versperren.

Allen Vorfällen der letzten Monate ist gemeinsam, dass sie nicht im rechtsfreien Raum stattgefunden haben, sondern dass 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 den Gesetzgeber, 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 zielgenau über neue Produkte zu informieren. Mehr als 80 Prozent aller Unternehmen in Deutschland nutzen Direkt-

marketing. Für den Mittelstand ist Direktmarketing sogar die einzige finanzierbare Werbeform.

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

3 §§ 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 3.4 und 3.5 dargestellt).

3.1 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 2007 ca. 72 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 zehntausende 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 – zehntausende Arbeitsplätze wären gefährdet. Gerade in der aktuellen, durch eine elementare Schwächung und Krise der Konjunktur geprägten Wirtschaftslage in Deutschland geht die Streichung des Listenprivilegs daher in eine völlig falsche Richtung.

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.

3.2 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.

3.3 Keine Vereinbarkeit mit der Richtlinie 95/46/EG

Hingewiesen sei auch darauf, dass die Abschaffung des Listenprivilegs keinesfalls von den Vorgaben der maßgeblichen Richtlinie 95/46/EG gedeckt wäre und deren Spielräume deutlich überschreitet. Ausführlich dargelegt wird dies in einem aktuellen Aufsatz, auf den insoweit daher hier Bezug genommen werden kann[1].

[1] Breinlinger in RDV 2008, Heft 6, Seite 223 ff

3.4 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.
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 (Formulierungsvorschlag vgl. unten 3.5).

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.

In der Diskussion um den vorliegenden Gesetzentwurf sind auch der Ausbau der sog. „Robinsonliste“, eine Stärkung des Widerspruchsrechts und die Kennzeichnung der werblichen Ansprache (z. B. mit einer individuell vergebenen Nummer) als weitere Lösungsansätze vorgeschlagen worden. Alle drei Vorschläge sind nach Einschätzung des BITKOM überlegenswerte Elemente, da sie –im Gegensatz zu dem Inhalt des vorliegenden Entwurfs- in unmittelbarer Weise mit den Zielen des Gesetzgebungsvorhabens verzahnt werden können. Möglich wäre das, in dem man diese Elemente als übergreifende Regelungen ausgestaltet, aber vor allem auch durch die Nutzung

dieser Elemente als Teile einer Richtlinie, die der Maßstab für eine erfolgreiche Auditierung ist (s.o.).

Aus Sicht des BITKOM wäre es für eine Stärkung der Robinsonliste erforderlich, den Verstoß gegen die Robinsonliste mit Sanktionen für das Unternehmen zu verbinden. Bezüglich der Kennzeichnungspflicht mit dem Ziel, dem Verbraucher Transparenz über die Unternehmen zu verschaffen, die seine Daten erhoben und weitergegeben haben, zeigen Modelle in anderen europäischen Mitgliedsstaaten, dass eine Rückverfolgbarkeit durch die Kennzeichnung ermöglicht werden kann. So erhält beispielsweise in Österreich - in dem ebenfalls ein Listenprivileg existiert - jeder Datenverarbeiter eine siebenstellige Registernummer (DVR), die dann auf der Werbeaussendung anzugeben ist. Der Bürger hat mit der Nummer über ein zentrales Register die Möglichkeit, festzustellen von welcher Firma die Daten stammen und dort der Verwendung seiner Daten zu widersprechen[2]. Dieses Verfahren bietet ein Höchstmaß an Transparenz, ohne zugleich dem Direktmarketing die Grundlage zu entziehen

3.5 § 28 Absatz 3, Verarbeitung oder Nutzung für Zwecke des Adresshandels, der Werbung oder der Markt- oder Meinungsforschung

Als Folge der Streichung des Listenprivilegs wird in § 28 Abs. 3 S. 1 als Grundsatz eingeführt, dass die Verwendung personenbezogener Daten für Zwecke des Adresshandels, der Werbung oder der Markt- oder Meinungsforschung nur zulässig ist, wenn der Betroffene entsprechend den Vorgaben des neuen Absatzes 3a eingewilligt hat. Das ist eine durch das Schutzbedürfnis des Bürgers nicht gerechtfertigte Fehlentwicklung mit ganz erheblichen wirtschaftlichen Auswirkungen (dazu schon oben 3.1). Die drei Erlaubnistatbestände in Satz 2, die Ausnahmen von diesem Grundsatz ermöglichen, sind aufgrund ihrer mehrfachen tatbestandlichen Verengung keine Entlastung.

- Die Nr. 1-3 beziehen sich nur auf die Verwendung von listenmäßig zusammengefassten Berufs-, Branchen- oder Geschäftsbezeichnung, Name, Titel, akademischer Grad, Anschrift, Geburtsjahr; nicht aber auf alle personenbezogenen Daten,
- die Nr. 1-3 stehen unter dem Vorbehalt der „Erforderlichkeit“, was ein ebenso unbestimmtes wie sachfremdes Kriterium ist,
- in Absatz 3 Satz 3 und Satz 4 (sog. Beipackwerbung) ist durch die Beschränkung auf das Speichern bzw. die Nutzung eine Übermittlung ausgeschlossen.

Klarzustellen ist im Gesetz, dass die Nutzung und Übermittlung von Daten aus öffentlich zugänglichen Quellen weiterhin zulässig ist.

Schließlich ist nach den Regelungen des Abs. 3 künftig die sog. „Empfehlungswerbung“ (d.h. eine Form der postalischen Werbung, bei der die verantwortliche Stelle in ihrem Namen ausschließlich andere Produkte empfiehlt) nicht mehr zulässig. Warum diese Werbeform allerdings verboten wird, ist angesichts der Gesetzesbegründung zur Zulässigkeit der „Beipackwerbung“ nicht nachvollziehbar. Zutreffend wird in der Begründung ausgeführt, dass bei der Beipackwerbung die Transparenz der Datennutzung weitgehend gewahrt bleibt, da der Datennutzer für den Betroffenen erkennbar bleibt, z.B. zur Wahrnehmung des Widerspruchsrechts. Das gilt in gleicher Weise aber auch für die Empfehlungswerbung, da der Empfehlende dem Betroffenen als

[2] *Informationen unter http://www.dsk.gv.at/site/6297/default.aspx*

Nutzer der Daten ohne weiteres erkennbar ist. In der Konsequenz liegt es, auch die Empfehlungswerbung zuzulassen.

In der Gesamtschau können die ausnahmsweise zulässigen Möglichkeiten der werblichen Ansprache das Handlungsvakuum, das durch die Streichung des Listenprivilegs entsteht, nicht annähernd ausgleichen. Um auch zukünftig seriös und rechtskonform agierenden Unternehmen die elementar wichtige Gewinnung von Neukunden zu ermöglichen, sollte daher als weiterer Erlaubnistatbestand in § 28 Abs. 3 aufgenommen werden:

[…]

4. für Zwecke des Adresshandels, der Werbung oder der Markt- oder Meinungsforschung, wenn die Verarbeitung und Nutzung der Daten aufgrund von Konzepten oder informationstechnischen Einrichtungen erfolgt, die mit einem Datenschutzsiegel nach § 1 Absatz 1 Datenschutzauditgesetz gekennzeichnet sind.

Die folgenden Aspekte stellen die Eignung der Erlaubnistatbestände Nr. 1-3 über die oben genannten Punkte hinaus in Frage:

3.5.1 § 28 Abs. 3 S. 2 Nr. 1 BDSG, Werbung für eigene Angebote

Eine zu den oben genannten Einschränkungen zusätzlich vorgenommene tatbestandliche Verengung ist die Voraussetzung, dass die verantwortliche Stelle die zu verwendenden Daten im Wege der Erhebung nach § 28 Abs. 1 Satz 1 Nr. 1 selbst gewonnen hat (d.h. auf Grund der Zweckbestimmung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses).

Diese Voraussetzung entwertet nicht zuletzt auch die in Abs. 3 Satz 4 vorgesehene Möglichkeit der Fremdwerbung, da diese nicht mit übermittelten Daten vorgenommen werden kann.

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 der jetzigen Formulierung die Formulierung *„für eigene Werbezwecke“* oder aber *„Werbung für eigene Angebote und Angebote verbundener Unternehmen“* aufzunehmen und die Voraussetzung der eigenen Erhebung nach § 28 Abs. 1 Satz 1 Nr. 1 zu streichen.

3.5.2 § 28 Abs. 3 S. 2 Nr. 2 BDSG, Werbung gegenüber freiberuflich oder gewerblich Tätigen

Angesichts der Zielsetzung des Gesetzgebungsvorhabens ist es nicht erforderlich, geschäftliche Korrespondenz mit werblichem Charakter in Unternehmensverbünden (z.B. bei vergünstigten Mitarbeiterangeboten im Konzern) oder Werbung im Kontext der beruflichen Tätigkeit einzuschränken. Klargestellt werden muss 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. Die Regelung in Nr. 2 geht vor diesem Hintergrund in die richtige Richtung, die Formulierung „unter deren Geschäftsadresse“ ist jedoch nicht hinreichend klar, da sie als Verengung des Anwendungsbereichs verstanden werden könnte. Als Gegensatz zu der privaten Adresse sollte terminologisch stattdessen zum Beispiel auf die „berufliche Anschrift“ o. ä. abgestellt werden. Zudem müsste auch die Werbung gegenüber Mitarbeitern öffentlicher Stellen (z.B. Kommunen) möglich sein, was die jetzige Formulierung der Vorschrift nicht zulässt.

3.5.3 Einwilligung („opt-in“) verursacht erhebliche Rechtsunsicherheit

Der Kabinettsentwurf macht die Einwilligung des Betroffenen zur regelmäßigen Voraussetzung der Nutzung seiner Daten für die werbliche Ansprache durch Unternehmen. Die Regelung ignoriert jedoch die Rechtswirklichkeit. Die Gestaltung einer rechtskonformen Einwilligung ist bereits nach geltendem Recht mit erheblichen Unwägbarkeiten verbunden. Die Praxis zeigt, dass die Entscheidung, ob die gewählte Formulierung und Gestaltung der Einwilligung rechtswirksam ist, letztlich den Gerichten obliegt.

Vor überraschenden Ergebnissen schützt dabei weder ein sehr sorgfältiges Vorgehen des Verwenders noch das Einvernehmen mit den Aufsichtsbehörden. Dass eine untragbare Rechtsunsicherheit und Abmahnwellen die Folgen sind, hat sich in den vergangenen fünf Jahren immer stärker gezeigt.

Die Rechtsunsicherheit führt zudem zu einem unkalkulierbaren, wirtschaftlichen Risiko für die Unternehmen. Das Einholen von Einwilligungserklärungen ist mit hohen Kosten für die Unternehmen verbunden. Entscheidet ein Gericht nach einem jahrelangen Rechtsstreit, dass der Einwilligungstext nicht rechtskonform sei, hat das Unternehmen diese Kosten nutzlos aufgewendet. Letztendlich wird diese Rechtsunsicherheit dazu führen, dass Unternehmen kaum noch in Einwilligungserklärungen investieren werden. In der Konsequenz würde sich die Verfügbarkeit von Opt-In-Adressen im Markt dramatisch reduzieren und damit die werbetreibende Wirtschaft massiv belasten.

3.6 Datennutzung zu Werbezwecken und Koppelungsverbot, § 28 Abs. 3a und 3 b BDSG

Durch die neuen Absätze 3a und 3b werden mit dem Opt-in und dem Koppelungsverbot Elemente und Rechtsfiguren, die bislang ihren Platz vor allem im Telemediengesetz haben, in das BDSG als das allgemeine Auffanggesetz verortet. Problematisch ist insoweit, dass dadurch der ohnehin nicht immer klar abgegrenzte Anwendungsbe-

reich des BDSG im Verhältnis zum TMG und TKG in bedenklicher Weise weiter aufgeweicht wird. Im Interesse einer für den Rechtsanwender klaren Systematik und Rangfolge von speziellem Gesetz und allgemeiner Regelung sollte dieser Tendenz unbedingt entgegengewirkt werden.

Darüber hinaus schlägt sich deutlich in beiden Absätzen die Tendenz nieder, eine Datennutzung zu Werbezwecken immer weiter einzuschränken.

Bei vielen Unternehmen im Internet basiert das Geschäftsmodell darauf, dass sie ihre Dienste durch zielgerichtete Werbung finanzieren. Diese Geschäftsmodelle dürfen keinesfalls in eine Grauzone gerückt oder sogar diskriminiert werden. Dies würde nicht zuletzt eklatant dem Interesse des Verbraucher bzw. Nutzers widersprechen, der die Nutzung von kostenlosen, weil werbefinanzierten Diensten einem kostenpflichtigen Angebot vorzieht.

Wenn das Angebot kostenloser Dienste in Deutschland faktisch aber nicht mehr möglich ist, weil die Refinanzierbarkeit erschwert oder gar unmöglich wird, werden diese Unternehmen ihre Dienste einstellen oder aber aus dem Ausland anbieten – möglicherweise mit einem sehr niedrigen Datenschutzniveau.

Anlass des Gesetzgebungsverfahrens sind Missbräuche außerhalb der digitalen (Medien-)Welt. Das Ziel des Gesetzgebungsverfahrens ist vor allem, mehr Transparenz für den Bürger bzgl. der Erhebung und Nutzung seiner Daten zu schaffen. Insbesondere durch den neuen Abs. 3a werden aber Verschärfungen im Bereich der digitalen Medien geschaffen, die mit diesem Anlass und dieser Zielsetzung keinerlei Verbindung haben. Die Folge der Vorkommnisse außerhalb des Internets darf aber keinesfalls sein, dass Geschäftsmodellen im Bereich der digitalen Medien die Existenzgrundlage entzogen wird.

Im Einzelnen zu Abs. 3a und 3b:

3.6.1 Ausgestaltung der Einwilligung, § 28 Abs. 3a BDSG

Dass mit Absatz 3a die elektronische Einwilligung tatbestandliche Aufnahme in das BDSG findet, ist eine längst fällige Annäherung an die Realität bzw. die tägliche Praxis und daher eine begrüßenswerte Entwicklung. Die Neuregelung im BDSG umfasst die gleichen Voraussetzungen an die elektronische Einwilligung wie die Regelung des § 13 Abs. 2 TMG (so auch die Gesetzesbegründung). Insofern ist klarzustellen, dass das TMG als speziellere Norm für Telemedien Vorrang hat.

Unklar ist, wie die Unternehmen sicherstellen sollen, dass „der Betroffene den Inhalt jederzeit abrufen“ kann. Nur große Firmen können es sich leisten, für jeden Interessenten ein eigenes Profil mit Zugang durch E-Mail-Adresse und Passwort vorzuhalten. In der Regel ist der Kunde auch gar nicht daran interessiert, z. B. den Text seiner Einwilligung in den Bezug eines Newsletters nachzuprüfen.

Darüber hinaus ist auch im Kontext des § 28 Abs. 3a BDSG die Möglichkeit sicherzustellen, dass die Datenweitergabe in Unternehmensverbünden nicht an das vorherige Opt-in und die Voraussetzungen des Abs. 3a gebunden ist. Die Datenweitergabe ist bei internationalen Unternehmen schon wegen der komplexeren Gesellschaftsstrukturen 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 Abs. 3a in Unternehmensverbünden hingegen würden den Verbraucher eher verwirren und abschrecken.

Die komplexen und detaillierten Anforderungen, die die vorgeschlagene Fassung des Abs. 3a aufstellt, werden vor allem kleinere und mittlere Unternehmen ohne eine eigene Rechtsabteilung häufig überfordern. Um zu vermeiden, dass trotz bestem Willen vielfach unwirksame Einwilligungserklärungen formuliert und entworfen werden, sollte ein amtliches Muster erstellt werden, das von den Unternehmen unmittelbar oder als Vorbild genutzt werden kann.

3.6.2 Koppelungsverbot durch § 28 Abs. 3b BDSG

§ 28 Abs. 3 b BDSG stellt eine erhebliche Verschärfung des Koppelungsverbots, wie es bislang im TMG formuliert war, dar. Durch die Einfügung „ohne die Einwilligung“ in den Text des Koppelungsverbots aus dem TMG wird eine bedenkliche Änderung des Maßstabs hin zu einer marktweiten Betrachtung erreicht (so auch die Begründung zum Gesetzentwurf).Diese Verschärfung greift in sehr bedenklicher Weise in die Vertragsfreiheit ein. Dem Nutzer muss die Freiheit erhalten bleiben, sich bewußt auch für ein Angebot zu entscheiden, bei dem seine Daten zu Werbezwecken verwendet werden. Vielfach sieht der Nutzer, der kostenlos attraktive Dienste im Internet nutzt, die spezifische Werbung nicht als Einschränkung, sondern als Vorteil an, der gewünscht ist.

Zudem kann die neue Formulierung zu zufälligen und unangemessenen Ergebnissen und damit zu Rechtsunsicherheit führen und sie greift unzulässig in das Marktgeschehen ein. Hinzuweisen ist darauf, dass gleichartige Geschäftsmodelle keinesfalls als Ergebnis einer unterstellten Absprache unter den marktbeteiligten Unternehmen zu werten sind (in diese Richtung geht aber die Begründung zum Gesetzentwurf), sondern die Gleichartigkeit ist eine normale und häufig zu beobachtende Folge einer nachvollziehbaren und zulässigen Marktlogik.

Ein Beispiel: Drei Unternehmen bieten das gleiche Geschäftsmodell an und stellen damit insgesamt den relevanten Markt dar. Zwei der drei Unternehmen haben die Nutzung mit der Verwendung der Nutzerdaten verbunden, das dritte Unternehmen nicht. Möchte nun das dritte Unternehmen sein Geschäftsmodell im Zuge einer Marktangleichung ändern und ebenfalls die Daten seiner Nutzer verwenden können, würden automatisch alle drei Geschäftsmodelle plötzlich dem Koppelungsverbot unterfallen und wären unzulässig.

Das Koppelungsverbot darf nicht zu einer Verarmung der Angebotsvielfalt gegenüber dem Verbraucher führen; das wäre kontraproduktiv. Der ursprüngliche Sinn des Koppelungsverbots im TMG war und ist es, zu verhindern, dass ein einzelnes, marktbeherrschendes Unternehmen diese Quasi-Monopolstellung zu Lasten des Kunden

ausnutzt. Dieser Sinn wird mit der neuen Formulierung und im Kontext des BDSG vollständig und sachwidrig aufgegeben.

Schließlich ist die Formulierung des Koppelungsverbots aus Sicht des BITKOM auch unvollständig. Ausweislich der Begründung soll es nur bei Unternehmen mit marktbeherrschender Stellung greifen. Der Gesetzesformulierung lässt sich dies aber nicht entnehmen. Aus Sicht des BITKOM reicht der Verweis auf die Begründung des Gesetzes nicht aus, die marktbeherrschende Stellung des Unternehmens sollte ausdrücklich als Tatbestandsmerkmal aufgenommen werden.

4 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. In die richtige Richtung geht daher der spezifische Kündigungsschutz, den der Entwurf für die Zeit während und nach der Tätigkeit als betrieblicher Datenschutzbeauftragter formuliert. Letztlich wird dadurch aber vor allem die bestehende Rechtsprechung kodifiziert, so dass der Regelung eher deklaratorischer Charakter zukommt, soweit in Vollzeit beschäftigte Datenschutzbeauftragte betroffen sind.

Wichtig im Zusammenhang mit einem spezifischen Kündigungsschutz ist es nach Ansicht des BITKOM, dass für die Verträge, die mit externen Datenschutzbeauftragten abgeschlossen werden, Mindestlaufzeiten vorgeschrieben werden, um zu vermeiden, dass in den Unternehmen zur Umgehung des Kündigungsschutzes zukünftig nur noch auf externe Datenschutzbeauftragte zurückgegriffen wird. Eine Mindestlaufzeit der Bestellung eines externen Datenschutzbeauftragten von 5 Jahren erscheint angemessen.

5 Erweiterung des Bußgeldrahmens und Erhöhung der Bußgelder, § 43 BDSG

Sehr problematisch ist aus Sicht des BITKOM die Regelung des § 43 Abs. 3 Satz 2 und 3, da diese in der praktischen Anwendung erhebliche Unsicherheiten aufwerfen könnte. Unklar dürfte vielfach insbesondere bleiben, was konkret und wie hoch der „wirtschaftliche Vorteil“ ist und ob dieser kausal mit der Ordnungswidrigkeit verbunden ist („aus der Ordnungswidrigkeit gezogen“). Zudem ist diese Sanktion im Falle der nur fahrlässigen Verwirklichung unverhältnismäßig.

6 § 42 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.

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. Es fehlen in der Aufzählung auch so wichtige Daten wie Passworte. 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, 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. Für Telemedien müsste als lex specialis eine dem Medium angemessene und entsprechende Alternative zur Schaltung einer Anzeige als Wahlmöglichkeit formuliert werden, z. B. Veröffentlichung auf einer eigenen Internetseite, Emailversand oder Notice Boards im Internet.

7 § 47, Übergangsregelung

Wegen der erheblichen und umfassenden notwendigen Umstellungen in den Unternehmen ist eine Übergangsregelung erforderlich, die zum einen ausreichend Zeit lässt und zum anderen für die Dauer des Übergangs die im betroffenen Unternehmen vorhandenen Datenbestände schützt. Die im Kabinettsentwurf vorgeschlagene Regelung ist nicht ausreichend, denn sie führt nicht –wie die flüchtige Lektüre zunächst

nahelegt- zu einem Schutz für die Dauer von 36 Monaten, sondern dazu, dass vorhandene Datensätze nach dem 1. Juli 2009 nicht mehr wie bisher aktualisiert werden können und damit regelmäßig ihren Nutzen verlieren. Faktisch gelten also die neuen Anforderungen ab dem 1. Juli 2009.

Zudem bezieht sich die vorgeschlagene Regelung nur auf § 28 BDSG, nicht aber auf § 29 BDSG.

Eine Differenzierung müsste in der Übergangsregelung hinsichtlich der Daten getroffen werden, die in der Vergangenheit auf Grundlage des § 4a BDSG rechtmäßig erhoben worden sind. § 4a BDSG regelt nach Auffassung von BITKOM in ausreichender Weise die Voraussetzungen für eine datenschutzrechtlich wirksame und den schutzwürdigen Belangen der Betroffenen entsprechende Einwilligungserklärung. Dies gilt insbesondere auch für bisher im Wege des Opt-Out eingeholte Einwilligungserklärungen, deren Wirksamkeit der Bundesgerichtshof in seinem „Payback"-Urteil aus dem Jahr 2008 bestätigte. Zu berücksichtigen ist auch, dass Einwilligungserklärungen gemäß § 4a BDSG vielfach im Rahmen der Begründung dauerhafter Vertragsverhältnisse eingeholt wurden und die Unternehmen hierfür erhebliche Aufwendungen getätigt haben. Die Einwilligungserklärungen wurden dabei im Vertrauen darauf eingeholt, dass sie mit Erfüllung der gesetzlichen Anforderungen auch zukünftig Bestand haben.

Als Formulierung schlagen wir daher vor:

„§ 47, Übergangsregelung
Für die Verarbeitung und Nutzung von Daten gemäß §§ 28 und 29 sind diese Vorschriften in der alten Fassung bis zum 1. Juli 2012 weiter anzuwenden. Die §§ 28 Abs.3 Satz 1 und 28 Abs. 3a des Bundesdatenschutzgesetzes in der seit 01.07.2009 geltenden Fassung sind nicht auf die Verarbeitung und Nutzung personenbezogener Daten anzuwenden, soweit der Betroffene vor dem 01.07.2009 gemäß § 4a BDSG wirksam in deren Verarbeitung und Nutzung eingewilligt hat."

8 Datenschutzauditgesetz

Hinweisen müssen wir zunächst darauf, dass eine umfassende und vollständige Einschätzung der zukünftigen Situation anhand des vorliegenden Entwurfs nicht möglich ist, da 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 Einzelheiten der Antragstellung) gemäß § 16 der späteren Regelung durch Rechtsverordnungen überlassen bleiben.

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

8.1 Hintergrund

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.

8.1.1 Bedarf und Nutzen

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 Gütesiegels allein mit dem Hinweis auf einen möglichen Wettbewerbsvorteil 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 auditierter 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.

8.1.2 Keine Berücksichtigung des europäischen Kontexts

Die überwiegende Anzahl der in Deutschland ansässigen Unternehmen dürfte innerhalb der EU (oder darüber hinaus) grenzüberschreitend tätig sein. Das umfasst auch die Datenverarbeitung, die häufig ebenfalls nicht an den Landesgrenzen von Deutschland endet. Für diese Unternehmen wirft das jetzige Konzept des Auditgesetzes viele Fragen auf, für die der Entwurf keine Lösungen bereit hält. So bleibt zum Beispiel unklar, ob ein ausländischer Subunternehmer ebenfalls auditiert werden muss, bevor der Auftraggeber das Siegel bekommen kann – die Einschaltung von Subunternehmern / Auftragnehmern im Ausland ist heute aber in vielen Fällen Standard. Schon in den häufigen Fällen der Auftragsdatenverarbeitung durch Unternehmen im EU-Ausland bleibt der Entwurf des Auditgesetzes die Antwort schuldig, ob die Auditierung und Kontrolle auch im Ausland stattfindet und falls ja, welches Datenschutzrecht dabei zur Anwendung kommen würde.

Insgesamt zeigt dies, dass ein nationaler Ansatz mit den Gegebenheiten des heutigen Wirtschaftslebens nicht Schritt halten kann.

8.2. § 1, Maßstab und Gegenstand des Datenschutzaudits

8.2.1 Auditgegenstand

Gegenstände des Audits können gemäß § 1 des Entwurfs ein Datenschutzkonzept sowie informationstechnische Einrichtungen der beantragenden Stelle sein. Durch diese Terminologie wird das DSAG mit § 9a BDSG verzahnt. Diese Lösung ist nach Ansicht des BITKOM fragwürdig. Weder das BDSG noch das DSAG geben eine Legaldefinition des „Datenschutzkonzepts“ und die Definition der „informationstechnischen Einrichtung“ in Satz 1 Nr. 2 ist eng, so dass unklar bleibt, ob auch Verfahren und Produkte mögliche Auditgegenstände sein können, da sich dies nicht ohne Weiteres aus den Begriffen „Datenschutzkonzept“ und „informationstechnische Einrichtung“ ergibt.

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

„Anbieter von Datenverarbeitungsanlagen 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.“

Zudem müsste klargestellt werden, ob auch Auftragsdatenverarbeiter als „Anbieter von Datenverarbeitungsanlagen“ zu verstehen sind und sich daher auditieren lassen können. Denn für Unternehmen, die eine Auftragsdatenverarbeitung als Dienstleistung anbieten, könnte die Auditierung u. U. eine sinnvolle Option sein.

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.

8.2.2 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 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 informationstechnischen 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, z.B. ISO 27001-Zertifizierung.

8.2.3 Freiwilligkeit des Audits

Jedes Datenschutzaudit muss freiwillig sein. BITKOM begrüßt daher, dass der Entwurf in § 1 die Freiwilligkeit zugrunde legt und zum Ausdruck bringt. In diesem Zusammenhang weisen wir auf unseren Formulierungsvorschlag oben 8.2.1 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.

8.3 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.

Zu begrüßen ist daher die Möglichkeit für Kontrollstellen, bundesweit tätig zu sein. Für Unternehmen, die in unterschiedlichen Bundesländern aktiv sind, schafft das die er-

forderliche 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.

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

8.4 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 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 (§ 9) 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.

8.5 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.

8.6 Kontrollen, § 3

Aus § 3 resultieren für die Unternehmen erhebliche Unsicherheiten, da nicht ersichtlich ist, wie häufig ein Unternehmen kontrolliert wird, was ein Kontrollverfahren auslöst und wer die diesbezügliche Entscheidung trifft. Dies muss in der gesetzlichen Regelung klargestellt werden, wobei die Entscheidung in die Hand der verantwortlichen Stelle gelegt werden muss. Die konkrete Formulierung des § 3 erscheint uns ebenfalls problematisch. So ist zunächst unklar, warum Satz 1 eingeleitet wird durch *„Vorbehalt-*

lich einer Rechtsverordnung…". Systematisch wäre dies als Einschränkung zu verstehen, für die wir jedoch keinen Raum und Anlass sehen.

BITKOM begrüßt die ausdrückliche Einbeziehung des betrieblichen Datenschutzbeauftragten in die Durchführungen der Kontrollen durch § 3 S. 2 des Entwurfs. 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 Formulierung der Einbeziehung des betrieblichen Datenschutzbeauftragten ist jedoch 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. 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.

In systematischer Hinsicht müsste die Einbeziehung (zumindest auch) in § 4g BDSG entsprechende Berücksichtigung finden; in § 11 DSAG könnte Bezug genommen werden, damit die Aufgaben des betrieblichen Datenschutzbeauftragten nicht in verschiedenen Gesetzen geregelt sind.

8.7 § 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.

8.8 § 6, 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 sichergestellt werden muss, könnte der Kontrahierungszwang auch dann noch eingefügt 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 Sei-

ten 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.

8.9 § 7, 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.

Ebenso wenig nachvollziehbar ist die Regelung in Absatz 2. Hier läge es wesentlich näher, dass die Dauer der Untersagung an die Behebung des fraglichen Verstoßes gekoppelt wird.

8.10 § 9, 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.

8.11 § 5, Anforderungen an Kontrollstellen

Die systematische Trennung der Bereiche „Recht“ und „Informationstechnik“ in Absatz 3 des § 5 ist im Gesamtzusammenhang des Entwurfs ein systematischer Fremdkör-

per, er findet sich an keiner anderen Stelle im Gesetz. Wir halten diese Trennung daher für entbehrlich.

8.12 § 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 neun 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 z. B. die Anzahl der Vertreter der Länderaufsichtsbehörden auf zwei reduziert werden.

8.13 § 17 Bußgeldvorschrift

Da BITKOM die Unterrichtungspflicht des § 6 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.

8.14 § 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.

8.15 § 19, Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

Im Referentenentwurf war durch § 19 DSAG in begrüßenswerter Weise an die erfolgreiche Auditierung eine unmittelbare Privilegierung für das auditierte Unternehmen gebunden, da Erleichterungen bei der Informationspflicht vorgesehen wurden. Diese Vorschrift ist im Kabinettsentwurf gestrichen worden. Das ist nach Ansicht des BITKOM das falsche Signal. Um den Unternehmen einen greifbaren Anreiz zur Auditierung zu geben, sollte diese Vorschrift wieder eingeführt und durch weitere Vorschriften zu Erleichterungen bei der datenschutzrechtlichen Einbettung ergänzt wer-

den, z.B. durch die Erlaubnis zur Nutzung des Listenprivilegs u.a. (vgl. dazu schon oben 3.3 und 8.1).

8.16 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 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, bei denen das Produkt oder System nicht isoliert, sondern als eine von vielen Komponenten eines Gesamtsystems zum Einsatz kommt. Auch hier sind das Zusammenspiel der Komponenten und dessen datenschutzrechtliche Konformität dem Einfluss des einzelnen Herstellers entzogen.

ANLAGE 2

Beispiel für Adress-/Datenhandel

Ein legales Adressgeschäft läuft in etwa folgendermaßen ab: Ein Versandhändler für Naturwaren und -textilien möchte in Niedersachsen neue Kunden gewinnen. Da es ein teures Unterfangen wäre, sämtliche Haushalte in dem Bundesland anzuschreiben – obendrein wäre es wenig zielgerichtet und ergiebig, da viele Menschen angesprochen würden, die keine Affinität zu Natur-Mode-Kollektionen haben –, wendet sich das Unternehmen an einen Adressmakler. Zusammen überlegen beide, wie potenzielle Kunden des Naturwarenversenders aussehen könnten: Sie ernähren sich naturbewusst, verfügen über ein gehobenes Einkommensniveau und haben Interesse an Umweltthemen. Der Adressmakler wählt dann Adresslisten aus, die entweder auf eine naturbewusste Ernährung oder auf ein gehobenes Einkommen oder auf ein Interesse an Umweltthemen schließen lassen. Eine Liste enthält dabei immer nur eine Angabe über die Zugehörigkeit des Betroffenen zu dieser Personengruppe, eine Kombination verschiedener Merkmale zu einer neuen Liste erfolgt nicht. Der Adressmakler setzt sich dann mit dem jeweiligen Listeigner, beispielsweise mit einem Versender von Bioprodukten oder einem Verlag für Umweltschutzmagazine, in Verbindung und bittet diese um Erlaubnis, ihre Adresslisten für die jeweilige Marketingaktion zu nutzen. Der Makler filtert dann alle Adressdubletten heraus, löscht die mehrfach vorhandenen Adressen und streicht alle Personen, die nicht in Niedersachsen wohnen. Darüber hinaus filtert er alle Verbraucher heraus, die durch einen Eintrag in eine WkW-Liste (Will-keine-Werbung) oder die Robinsonliste signalisiert haben, dass sie keine postalische Werbung erhalten wollen. Die drei Listen („naturbewusste Ernährung“, „gehobenes Einkommen“ und „Interesse an Umweltthemen“) werden einzeln im Rahmen der Auftragsdatenverarbeitung an einen Lettershop weitergegeben, der vom Naturwarenhändler das zu versendende Werbematerial, also das Werbeschreiben, den Katalog u.ä. und vom Listbroker die drei Adressenlisten des Listbrokers erhält und dann das Werbematerial versendet. Letztendlich bekommen nur die Personen Post, die auf mindestens einer der drei Listen stehen, welche nach den Wünschen des Naturwarenhändlers ausgewählt wurden, und von denen mit einer gewissen Wahrscheinlichkeit davon ausgegangen werden kann, dass sie sich für die Angebote interessieren. Dieses Verfahren reduziert die Streuverluste in der Neukundenwerbung und spart somit Geld und schont zudem Ressourcen, da die Briefe zielgerichtet zugestellt werden und anfallendes Altpapier auf ein Minimum reduziert wird.

Aus datenschutzrechtlicher Sicht ist der Umstand von elementarer Bedeutung, dass bei diesem Geschäftsprozess der Kunde des Adressmaklers, in diesem Fall der Naturwarenversender, die drei Listen, die bei einem neutralen Dienstleister verarbeitet werden, nie zu Gesicht bekommt, sondern nur dann die Daten der Verbraucher erhält, wenn diese sich auf seine Werbung hin direkt bei ihm melden. Zudem ist ein direkter Rückschluss auf das Kaufverhalten eines einzelnen Kunden ausgeschlossen.

Beispiel für Direktmarketing

Direktmarketing ist insbesondere für die vier Millionen kleinen und mittelständischen Unternehmen, z.B. Handwerksbetriebe (Optiker, Goldschmiede/Juweliere etc.) eine attraktive, weil wirkungsvolle und wirtschaftliche Werbeform. Wenn ein Optiker in seinem Einzugsgebiet beispielsweise die Interessenten für höherwertige Brillengläser ansprechen will, so bietet Direktmarketing dazu optimale Ansatzpunkte. Bei einer generellen Opt-In-Lösung wäre der Optiker aufgrund mangelnder Datenverfügbarkeit zunächst darauf beschränkt, nur seine Bestandskunden ansprechen zu können. Neukundenakquise wäre auf diese Weise kaum noch möglich. Andere Werbeformen, wie beispielsweise Postwurfsendungen oder Anzeigen in lokalen Medien, funktionieren bei Unternehmen ohne bekannten Markennamen nur bedingt. Den Aufbau einer Marke kann sich ein solches Unternehmen aber nicht leisten. Händlernetze und Geschäfte, die auf Franchisingmodellen basieren, könnten kaum noch zentrale Direktmarketingaktivitäten durchführen, da die Adressen von Bestandskunden jeweils den einzelnen lokalen Einheiten zugeordnet sind und ein Opt-In derzeit nur in den seltensten Fällen vorliegt.