

02. März 2009

Verbrauchersouveränität im Datenschutz herstellen

**Stellungnahme
des Verbraucherzentrale Bundesverbandes**

**zum Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur
Änderung datenschutzrechtlicher Vorschriften vom 10. Dezember 2008**

Verbraucherzentrale Bundesverband e.V. – vzbv
Fachbereiche Wirtschaft und Internationales
Markgrafenstr. 66
10969 Berlin
wirtschaft@vzbv.de
www.vzbv.de

Gesamtwürdigung

Die **Datenschutzskandale** der vergangenen Monate haben eindringlich vor Augen geführt, dass die **Datenschutzvorschriften** Verbraucher **unzureichend vor einem Missbrauch ihrer Daten schützen**. Binnen 44 Stunden und für 850 Euro konnte der Verbraucherzentrale Bundesverband im vergangenen Sommer 6 Millionen Datensätze erwerben, bei denen 4 Millionen Datensätze Kontoverbindungen enthielten.ⁱ Dieser Skandal wurde im Dezember 2008 sogar noch einmal übertroffen, als der *Wirtschaftswoche* Datensätze inklusive Kontonummern von 21 Millionen Bürgern angeboten wurden. Die Deutsche Telekom AG musste zudem nicht nur eingestehen, Vorstände, Aufsichtsräte und Journalisten bespitzelt zu haben, sie musste auch Recherchen des *Spiegels* Recht geben, wonach Kopien von 17 Millionen Kundendatensätzen der Telekomtochter T-Mobile bereits 2006 in die Hände Unbefugter gelangten. Kurz vor Weihnachten erfuhr die Öffentlichkeit zudem, dass die Landesbank Berlin sensible Transaktionsdaten ihrer Kreditkartennutzer völlig ungeschützt an Dienstleister verschickte. Unzureichend fallen auch die Sanktionen bei Verstößen gegen das Datenschutzrecht aus. So betrug das Bußgeld, das gegen den Datenhändler verhängt wurde, der dem Verbraucherzentrale Bundesverband 6 Millionen Daten für 850 Euro verkaufte, gerade einmal 900 Euro.

Diese Beispiele zeigen, dass nicht nur unseriöse „schwarze Schafe“, wie einige Branchenverbände argumentieren, sondern auch große namhafte Unternehmen es versäumen, Verbraucherdaten ausreichend zu schützen, es unterlassen, Millionen von Verbrauchern über einen Datenklau zu informieren und für weniger als tausend Euro Millionen Adressen und sogar Kontonummern auf dem freien Markt gekauft werden können. Diese Beispiele verdeutlichen den **gravierenden Handlungsbedarf im Datenschutz**. Der Präsident des Bundesverfassungsgerichts, Prof. Dr. Dres. h.c. Hans-Jürgen Papier, mahnte im Dezember 2008 denn auch im Rahmen einer Veranstaltung zum 25. Jahrestag des Volkszählungsurteils in Richtung Politik, dass das Grundrecht auf informationelle Selbstbestimmung den Staat dazu verpflichte „angemessene Schutzregime“ zu errichten. Und er forderte, dass „sich der Staat nicht mit bloßen Selbstverpflichtungen Privater begnügen dürfe, sondern [dass der Staat] selbst eine verbindliche Ordnung konstituieren müsse“. **Ziel** einer Novellierung des Bundesdatenschutzgesetzes muss es daher sein, die **Verbrauchersouveränität im Datenschutz herzustellen**.

Defizite bestehen insbesondere in **vier Bereichen**:

- § **Durch das Listenprivileg** werden bestimmte Daten über **Verbraucher auch ohne deren Einwilligung und Wissen** für Werbe- und Marketingzwecke verkauft und vermietet. Während **Unternehmen Geld** mit den Daten der Verbraucher **verdienen**, können **Verbraucher keine Kontroll- und Steuerungsfunktion** über die Verwendung ihrer Daten **ausüben**.
- § Wenn Einwilligungen in die Datenverarbeitung zu Werbe- und Marketingzwecken eingeholt werden, können diese von Verbrauchern häufig nicht bewusst erteilt werden, da sie **schwer- oder missverständlich formuliert sind**ⁱⁱ oder aber der Zugang zu einem gewerblichen Angebot davon abhängig gemacht wird, dass Verbraucher in die Datennutzung zu Werbezwecken einwilligen (**Koppelungsgeschäft**).
- § Die Daten sind unzureichend vor unbefugtem Kopieren, Weitergabe und Verarbeitung geschützt (**mangelnde Datensicherheit**). – So konnten Call-

Center-Mitarbeiter beispielsweise ohne große Hürden Kopien von Datenbeständen fertigen.

- § **Sanktionen** gegen Datenschutzvergehen sind **zu lasch**, **Verbraucherverbände können ihre kollektiven Klagerechte nur bedingt einsetzen**, die **Überwachung durch die Aufsichtsbehörden ist personell unterbesetzt** und **Anreize** für einen verbraucherfreundlichen Umgang mit personenbezogenen Daten sind **unzureichend**.

Die Bundesregierung hat auf die Datenschutzskandale der letzten Monate mit dem Entwurf eines *Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften* vom 10. Dezember 2008 prompt reagiert.ⁱⁱⁱ Der Entwurf stellt durch die **Abschaffung des Listenprivilegs**, die **Einführung von Anforderungen an Einwilligungen (Opt-In)** und die **Einführung von Informationspflichten bei Datenschutzverstößen und -pannen** einen **notwendigen ersten Schritt in die richtige Richtung** dar. Der Entwurf **beendet die bestehende Rechtslage**, wonach **der Widerspruch und nicht die Einwilligung die Regel bei der Datenverarbeitung zu Werbe- und Marketingzwecken darstellt**. Auch wird eine **längst überfällige Grundlage** für ein **Datenschutzaudit** geschaffen. Das Datenschutzaudit kann als marktwirtschaftliches Instrument einen wichtigen Anreiz für eine bessere Datenschutzpraxis darstellen.

Nachdem die **Bundesländer** den Gesetzentwurf insgesamt **positiv gewürdigt** und eine **Reihe von verbraucherfreundlichen Nachbesserungen angeregt** haben, kommt es im **parlamentarischen Verfahren** darauf an, die **vorgesehenen Maßnahmen nicht zu verwässern**, sondern den Entwurf **zügig zu verabschieden**. **Allerdings sollte an entscheidenden Stellen nachgebessert werden:**

Erstens muss an der Abschaffung des Listenprivilegs grundsätzlich festgehalten werden. Es müssen allerdings **Ausnahmen** bei der Abschaffung des Listenprivilegs überarbeitet und teilweise rückgängig gemacht werden. Einige der Regelungen für die Verwendung von Daten für eigene Werbung widersprechen Vorschriften in der europäischen Datenschutzrichtlinie und im Gesetz gegen den unlauteren Wettbewerb (UWG). Hier gilt es daher, die Regelungen an bestehende Vorschriften anzugleichen. Zudem sollte die Ausnahme, nach der listenförmige Daten weiterhin zum Zwecke der Spendenwerbung genutzt werden können, an Kriterien geknüpft werden.

Zweitens ist in § 28 Abs. 3b BDSG-E ein **generelles Koppelungsverbot** einzuführen. Das von der Bundesregierung vorgeschlagene eingeschränkte Koppelungsverbot ist - wie auch der Bundesrat betont - unzureichend.

Drittens ist die **Einführung von Informationspflichten** bei Datenschutzverstößen und -pannen zwar **grundsätzlich zu begrüßen**. Allerdings sollten die Informationspflichten **auch für öffentliche Einrichtungen gelten**, sie **dürfen nicht** auf die Fälle beschränkt werden, in denen von einer **schwerwiegenden Beeinträchtigung der Betroffenen auszugehen ist** und die **Information sollte immer direkt an die Betroffenen gehen**.

Viertens sind die **Bußgeldtatbestände** in § 43 BDSG noch weiter als vorgesehen **auszuweiten**.

Fünftens ist die **Übergangsfrist** für die Umsetzung der neuen Regelungen **von drei Jahren unplausibel und zu lang**. Die Datenschutzskandale haben gezeigt, dass der

Handlungsbedarf heute besteht. **In Abwägung von Verbraucher- und Wirtschaftsinteressen sollte eine Einjahresfrist ausreichen.**

Sechstens sind noch eine Reihe weiterer Maßnahmen zu ergreifen, die nicht im Gesetzentwurf vorgesehen sind. Diese umfassen die **Einführung eines Sammelrückrufs für Einwilligungen, Maßnahmen zur Verbesserung der Datensicherheit, die Einführung von Kennzeichnungs- und Protokollierungspflichten, die Stärkung des kollektiven Rechtsschutzes, eine bessere personelle Ausstattung der Datenaufsichtsbehörden und der Ausbau der Eingriffsbefugnisse für die Aufsichtsbehörden.**

Siebtens ist es zwar zu begrüßen, dass ein Entwurf eines Datenschutzauditgesetzes vorgelegt wurde, es greift an entscheidenden Stellen jedoch zu kurz. Zu **kritisieren** ist insbesondere, dass die Aufsichtsbehörden kein Recht erhalten, auch die Gutachten der Kontrollstellen zu überprüfen um ggf. eine Zulassung zu entziehen und dass in **dem neuen Datenschutzauditausschuss nicht die Mitwirkung von Verbrauchervertretern vorgesehen** ist, die Mitwirkung der Anbieter hingegen schon.

Es ist notwendig, dass der Entwurf **zügig im Sinne** der Verbraucher **verbessert und verabschiedet** wird. Allerdings bedarf ein effektiver Datenschutz nicht lediglich guter Gesetze, sondern auch eines **wirksamen Vollzugs**. Da der Vollzug im Wesentlichen Ländersache ist, stehen die **Bundesländer in der Pflicht**, ihre **Aufsichtsbehörden und die Verbraucherorganisationen** so auszustatten, dass diese ihren **Aufgaben gerecht werden können**.

1. Bewertung des Entwurfs eines Gesetzes zur Änderung datenschutzrechtlicher Vorschriften

Zu Artikel 2 Nr. 1a neu (§ 4 Abs. 3 Satz 1 BDSG)

In § 4 BDSG werden die Zulässigkeiten der Datenerhebung, -verarbeitung und -nutzung geregelt. In der Praxis hat sich insbesondere § 4 Abs. 3 Satz 1 BDSG als problematisch erwiesen. Die **bisherigen Einschränkungen** „sofern er nicht bereits auf andere Weise Kenntnis erlangt hat“ und „die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalls nicht mit der Übermittlung an diese rechnen muss“ **haben dazu geführt**, dass die **Informationspflicht der verantwortlichen Stelle über die Erhebung der Daten gegenüber den Verbrauchern ein Ausnahmefall, anstatt wie intendiert die Regel darstellte**. Diese Informations- und Dokumentationspflichten sind jedoch essentiell für Verbraucher, damit sie wissen, von wem und für welche Zwecke die Daten erhoben und an welchen Empfängerkreis sie weitergegeben werden.

Daher sollten diese Einschränkungen ersatzlos gestrichen werden. Diese Forderung wird u.a. auch vom Bundesrat erhoben.^{iv} Die Zurückweisung dieser Forderung durch die Bundesregierung in ihrer Gegenäußerung mit dem Argument, dass sich die Novellierung auf „grundlegende Änderungen“ beschränken sollte, überzeugt nicht. Denn das Gesamtziel der Novellierung muss darin bestehen, für ein Mehr an Transparenz über die Verwendung von personenbezogenen Daten zu sorgen. Die hier angeregte Änderung würde hierzu einen Beitrag leisten.

Zu Artikel 2 Nr. 2 (§ 4f Abs. 3 BDSG)

Betriebliche Datenschutzbeauftragte können einen wichtigen Beitrag für einen effektiveren Datenschutz leisten, indem sie die Einhaltung gesetzlicher Vorschriften kontrollieren und Verbesserungen im Bereich des Datenschutzes forcieren.

Notwendig ist jedoch, dass diese ihrer Arbeit ohne Angst vor einer Kündigung nachgehen können und über ausreichende Fachkenntnisse verfügen. Das derzeitige Benachteiligungsverbot des § 4f BDSG sichert die Unabhängigkeit des Datenschutzbeauftragten und seiner fachlichen Kompetenz nur unzureichend.

Der Entwurf sieht vor, Datenschutzbeauftragte mit einem Kündigungsstatus vergleichbar mit dem von Immissionsschutzbeauftragten oder Betriebsratsmitgliedern auszustatten. Auch erhalten die Datenschutzbeauftragten ein Anrecht auf Fortbildung und deren Finanzierung. Da die Maßnahmen die Stellung des Datenschutzbeauftragten stärken und seine Fachkunde verbessern, **begrüßen wir die Vorschläge ausdrücklich.**

Zu Artikel 2 (§ 11 Abs. 2 Satz 2 und 4 BDSG)

Die **Datenschutzskandale** haben eindringlich gezeigt, dass **Defizite in der Auftragsdatenverarbeitung** existieren und die **Datensicherheit häufig unzureichend kontrolliert wird**. Daher ist es **zum einen** erforderlich, die Anforderungen an die Auftragsdatenverarbeitung in § 11 Abs. 2 Satz 2 BDSG zu präzisieren. Die Datenschutzaufsichtsbehörden stellen wiederholt fest, dass eine Auftragsverarbeitung häufig nicht schriftlich erteilt wird oder der Auftrag keine schriftlichen Regelungen hinsichtlich der Datenerhebung, -verarbeitung oder -nutzung, der technischen und organisatorischen Maßnahmen oder etwaiger Unterauftragsverhältnisse enthält. Zudem können die verantwortlichen Stellen regelmäßig nicht dokumentieren, dass Einwilligungen von Verbrauchern in die Datenverarbeitung vorliegen oder aber es werden veraltete Einwilligungen von Verbrauchern vorgezeigt.

Daher sollte der Gesetzgeber die Vorgaben **dahingehend präzisieren**, dass die der Norm unterworfenen nichtöffentlichen Stellen die **gesetzlichen Anforderungen besser erkennen können**. Ziel muss sein, dass bei der Auftragsdatenverarbeitung die Datenverarbeitung und -nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse schriftlich geregelt sind. Diese Vereinbarungen sollten auch generelle Weisungen in Bezug auf die einzelnen Verarbeitungsschritte und insbesondere der Löschung bzw. Rückgabe der Daten an den Auftraggeber, die Datensicherung und die Vergabe von Unteraufträgen enthalten.

Zum anderen sollte in § 11 Abs. 2 Satz 4 BDSG die **Häufigkeit, Tiefe und Dokumentation von Kontrollen bei den Auftragsdatenverarbeitern durch den Auftraggeber näher geregelt werden**. Die Praxis der Datenschutzaufsicht zeigt, dass diese vorgeschriebenen Kontrollen nicht in der gebotenen Häufigkeit und Qualität durchgeführt werden. Dies ist insbesondere dann problematisch, wenn Verbraucherdaten unterschiedlicher Herkunft bei einem Unternehmen (wie einem Call-Center) liegen. Wenn hier nicht ausreichend kontrolliert wird, besteht eine hohe Missbrauchsgefahr darin, dass die Daten unberechtigt miteinander verknüpft werden.

Zu Artikel 2 Nr. 5 (§ 28 BDSG)

Zu c) und d) (Abschaffung des Listenprivilegs)

Das **Hauptziel** der Änderungen in c) und d) besteht in der **Streichung** des bisher in § 28 Abs. 3 Satz 1 Nr. 3 BDSG geregelten **Listenprivilegs**. Beim Listenprivileg handelt es sich um ein Privileg, das auf die 1970er Jahre zurück geht. Es sieht vor, dass Unternehmen personenbezogene Daten verkaufen oder „vermieten“ dürfen so lange es sich bei diesen Daten im Wesentlichen um Adressdaten und einen weiteren Datenpunkt handelt (Schnäppchenjäger, BMW-Fahrer, treuer Kunde).

Ein Privileg, das vor 30 Jahren kaum zu rechtfertigen war, hat heute durch die Zunahme der Datenverarbeitungskapazitäten dazu geführt, dass die **Verbrauchersouveränität auf den Kopf gestellt wird**. Denn Daten werden ohne Zustimmung und Wissen der Verbraucher verkauft oder „vermietet“ und es besteht die Gefahr, dass die Daten zu umfassenden Profilen kombiniert werden. Sie erhalten Werbung von Unternehmen, mit denen sie bislang nicht zu tun hatten und eventuell auch kein Kontakt haben wollen. Das **Listenprivileg widerspricht** demnach dem – der Verbraucherpolitik zu Grunde liegenden – **Leitbild des mündigen Verbrauchers**, der selbst entscheidet, wem er welche seiner Daten zur Verfügung stellt. – In einer aktuellen Umfrage von Infratest dimap sprachen sich 95 Prozent der Befragten denn auch für eine Einwilligungslösung für die Datenweitergabe aus.^v

Die **Abschaffung des Listenprivilegs** stellt daher aus drei Gründen einen **wesentlichen Baustein für eine Verbesserung des Datenschutzes** dar:

1. Die **Verbrauchersouveränität** wird im Datenschutz **gestärkt** – die Verbraucher werden Souverän über ihre Daten. Verbraucher können selbst entscheiden, ob mit ihren Daten Geld verdient werden darf und ob sie an Dritte gehen dürfen.
2. Die **Prävention** wird im Datenschutz **verbessert** – je weniger Daten erhoben und übermittelt werden, desto weniger können sie in Profilen zusammengefasst und ggf. missbraucht werden.
3. Verbraucher **werden weniger** durch unverlangte **Werbung** in ihren Briefkästen **belästigt**. – Nach einer Umfrage von Infratest dimap fühlen sich 82 Prozent der Befragten durch Werbeanrufe und -briefe belästigt.^{vi}

Aus diesen Gründen **begrüßen wir die Neufassungen der Absätze 2 und 3 grundsätzlich. Allerdings sehen die Vorschläge Ausnahmen vor, die aus Verbrauchersicht als kritisch zu bewerten sind.**

Erstens darf die neue Regelung nicht als Freibrief für jedwede – unter Umständen auch unverlangte – Kontaktaufnahme zum Verbraucher gelten. Zwar ist die Kontaktaufnahme zu Werbezwecken grundsätzlich von den Spezialvorschriften des Gesetzes gegen den unlauteren Wettbewerb (UWG) abgedeckt. Dennoch sind Fallkonstellationen denkbar, in denen eine **Regelungslücke** besteht. So heißt es in der amtlichen Begründung zum Entwurf eines Ersten Gesetzes zur Änderung des Gesetzes gegen den unlauteren Wettbewerb der Bundesregierung vom 20.08.2008 (DS 16/10145, Seite 21): „Weltanschauliche, wissenschaftliche, redaktionelle oder verbraucherpolitische Äußerungen von Unternehmen oder anderen Personen unterfallen weiterhin nicht dem UWG, soweit sie in keinem objektiven Zusammenhang mit dem Absatz von Waren [...]“.

stehen. Dienen sie nur der Information der Leserschaft oder der die Anonymität der befragten Personen währenden Markt- und Meinungsforschung, fehlt es an einem objektiven Zusammenhang zum Warenabsatz, so dass eine geschäftliche Handlung (im Sinne des UWG) nicht vorliegt.“

Danach sind sowohl Werbeansprachen, aber dezidiert auch Befragungen der Markt- und Meinungsforschung nicht vom UWG erfasst, soweit diese nicht in einem objektiven Zusammenhang zum Warenabsatz stehen und damit auch keine geschäftliche Handlung sind.

An dieser Stelle entsteht allerdings ein Wertungswiderspruch zwischen den Regelungen des UWG und des BDSG: Werbeansprachen im Sinne des § 7 Abs. 2 UWG setzen für den Bereich der Werbung in elektronischer Form (E-Mail, SMS) und per Fax grundsätzlich eine ausdrückliche Einwilligung des Verbrauchers voraus. Das gleiche gilt für die aktuell diskutierte Novellierung des UWG in dem Punkt Telefonwerbung. Ausgehend von dem Schutzzweck dieser Regelungen, Verbraucher vor der unverlangte Kontaktaufnahme zu Werbezwecken und Verbraucher vor derartigen Belästigungen zu schützen, findet sich zu der geplanten Vorschrift im BDSG ein Widerspruch. Die nach dem UWG erforderliche *ausdrückliche* Einwilligung für eine Werbeansprache findet sich derzeit nicht in § 28 Abs. 3 Satz 1 BDSG-E wieder. Das hat zur Folge, dass die Kontaktaufnahmen zu Zwecken der Markt- und Meinungsforschung auch dann möglich sind, wenn der angerufene Verbraucher zuvor nicht ausdrücklich eingewilligt hat. Ausgehend von dem Belästigungsgrad des Verbrauchers lässt sich eine thematische Differenzierung nach einer zielgerichteten Werbeansprache im Sinne des UWG und einer Ansprache zu Zwecken der Meinungsforschung im Sinne des BDSG sachlich nicht rechtfertigen. Daher muss in § 28 Abs. 3 Satz 1 BDSG-E klargestellt werden, dass es der **ausdrücklichen** Einwilligung bedarf.

Zweitens ist die **Regelung in der neuen Nummer 1 in Absatz 3 BDSG-E unzureichend**. Hier wird geregelt, dass personenbezogene Daten für Zwecke der Werbung verarbeitet oder genutzt werden können, wenn die Verarbeitung oder Nutzung für Zwecke der Werbung für *eigene* Angebote oder der *eigenen* Markt- oder Meinungsforschung erfolgen soll.

Zum einen ist die Regelung aus dem Grund problematisch, da die Verarbeitung oder Nutzung für Zwecke der Werbung nicht beschränkt wird auf eigene *ähnliche* Produkte und Dienstleistungen. Damit widerspricht die vorgeschlagene Regelung sowohl der europäischen Datenschutzrichtlinie als auch dem UWG. In der Datenschutzrichtlinie heißt es in Artikel 13 Nr. 2:

„eine natürliche oder juristische Person“ kann, „wenn sie von ihren Kunden im Zusammenhang mit dem Verkauf eines Produkts oder einer Dienstleistung ... deren elektronische Kontaktinformationen für elektronische Post erhalten hat, diese zur Direktwerbung für *eigene ähnliche* Produkte oder Dienstleistungen verwenden, sofern die Kunden klar und deutlich die Möglichkeit erhalten, eine solche Nutzung ihrer elektronischen Kontaktinformationen bei deren Erhebung und bei jeder Übertragung gebührenfrei und problemlos abzulehnen“

In § 7 Abs. 3 Nr. 2 UWG findet sich eine ähnliche Regelung, die die Werbung unter Verwendung elektronischer Post (E-Mail und SMS-Werbung) auf *eigene ähnliche* Waren oder Dienstleistungen beschränkt. **Daher** sollte in der Nummer 1 des Absatzes 3 **klargestellt werden**, dass eine **Verarbeitung und Nutzung ausschließlich für Zwecke der Werbung für eigene *ähnliche* Angebote erlaubt ist**.

Zum anderen ist zu präzisieren, dass die Voraussetzung für Werbung nur so lange existiert, wie das Geschäftsverhältnis besteht. Nur weil ein Verbraucher einmal eine Kiste Wein bei einem Weinhändler bestellt, rechtfertigt diese Bestellung keine kontinuierliche Werbung.

Was die **Ausnahmeregelung für steuerbegünstigte Spendenwerbung** angeht, so **lehnen** wir eine privilegierte Behandlung ohne weitere Voraussetzungen **für solche Zwecke ab**. Es ist empirisch nicht erwiesen, dass Spendenorganisationen verantwortungsvoller als Unternehmen mit personenbezogenen Daten umgehen. Da jedoch grundsätzlich ein öffentliches Interesse an Spendentätigkeit besteht, kann die Ausnahmeregelung unter der **Voraussetzung akzeptiert werden**, dass die **Spendenorganisationen zum einen ein Datenschutzaudit** durchgeführt haben **und zum anderen über ein Spendensiegel des Deutschen Zentralinstituts für soziale Fragen (DZI) verfügen oder Mitglied des Deutschen Spendenrats e.V. sind**.

Die **Abschaffung des Listenprivilegs** wird von einigen Wirtschaftsverbänden **scharf kritisiert**. Vorgetragen wird, dass die Abschaffung des Listenprivilegs die Direktwerbung de facto unmöglich mache, tausende Arbeitsplätze gefährde, Verbraucher nicht mehr für sie interessante Werbung erhielten und Unternehmen als Reaktion wieder mehr ungezielte Werbung versenden müssten, wodurch nicht nur Kosten entstünden, Verbraucher belästigt würden, und schlussendlich auch die Umwelt belastet würde.^{vii} So wird beispielsweise behauptet, dass die Abschaffung des Listenprivilegs dazu führen würde, dass Verbraucher keine Nachrichten mehr über aktuelle Sonderkonditionen für den Kauf eines neuen Autos oder keine Informationen über Kennenlern-Wochenenden des neu eröffneten Fitnessclubs erhielten.^{viii}

Die **Kritik der Wirtschaftsverbände ist überzogen**:

- § Auch nach einem Wegfall des Listenprivilegs wird Werbung weiterhin über die unterschiedlichsten Kanäle möglich sein. Angefangen bei der Anzeigen-, Radio-, TV-, Internet- und Plakatwerbung bis hin zur Beilagen-, Empfehlungs- oder auch Briefkastenwerbung. Selbst die adressierte Direktwerbung wird nach Streichung des Listenprivilegs möglich sein – auf der Grundlage eines bestehenden Geschäftsverhältnisses oder einer Einwilligung. Diese Beispiele verdeutlichen, dass Unternehmen Verbraucher auch weiterhin über Angebote oder neue Produkte informieren können.
- § Werbung wird – und das bestätigen die Wirtschaftsverbände selbst – auch weiterhin verschickt werden. Daher sind Warnungen vor massiven Arbeitsplatzverlusten wenig überzeugend. Im Gegenteil: Durch die Abschaffung des Listenprivilegs entsteht ein Markt für Daten mit Einwilligung, der betreut werden muss. Daher werden Werbe-, Dialogmarketing- und Kreativagenturen, Listbroker, Druckereien und Postdienstleister auch weiterhin gebraucht – allerdings werden die Rahmenbedingungen zugunsten der Verbraucher gesteckt. So weist ein aktueller Artikel in der Fachzeitschrift *direkt marketing* darauf hin, dass „neue Ansätze [im Direktmarketing ohnehin] zwingend notwendig“ sind. Und kritisch wird hinterfragt, „ob die eingefahrenen postalischen Wege,

gemessen an Aufwand und Response, tatsächlich so erfolgreich waren, wie man dies nun versucht zu kommunizieren“.^{ix}

Zu e) (Opt-In und Koppelungsverbot)

Hauptziele der Änderungen in e) liegen in der Definition von Anforderungen an Einwilligungen (Abs. 3a) und der Einführung eines begrenzten Koppelungsverbots (Abs. 3b). Wir **begrüßen** es sehr, dass **eine Einwilligung nur wirksam** sein soll, wenn der Betroffene durch **Ankreuzen**, durch eine **gesonderte Unterschrift** oder ein anderes, ausschließlich auf die Einwilligung in die Weitergabe seiner Daten für Werbezwecke bezogenes Tun zweifelsfrei zum Ausdruck bringt, dass er die Einwilligung bewusst erteilt. Der Verbraucherzentrale Bundesverband fordert schon seit Jahren die Festschreibung eines solchen ‚Opt-Ins‘ für Einwilligungen.

Die **vorgeschlagene Formulierung** sollte jedoch noch **verbessert und hierdurch verdeutlicht werden**, dass Hinweispflichten des § 4a Abs. 1 Satz 2 BDSG entsprechend gelten. Daher sollte im Absatz 3a BDSG-E ergänzt werden: „bezüglich der Hinweispflichten gilt § 4 a Abs. 1 Satz 2 BDSG entsprechend“. Zudem sollte im Satz 2 das „Ankreuzen“ durch ein „gesondertes Ankreuzen“ ersetzt werden – hierdurch wird die Anforderung noch klarer und konsistent mit der folgenden Anforderung an eine „gesonderte Unterschrift“.

In Abs. 3b wird ein **eingeschränktes Koppelungsverbot** eingeführt. Zwar stellt die vorgeschlagene Regelung einen Fortschritt im Vergleich zu den Regelungen des Telekommunikationsgesetzes und des Telemediengesetzes dar, allerdings greift der **Vorschlag weiterhin zu kurz**. Problematisch ist insbesondere, dass das Koppelungsverbot nur für marktbeherrschende Unternehmen gelten soll. Diese Intention wird durch eine Zumutbarkeitsregelung umgesetzt. Zwei Beispiele illustrieren die Schwäche dieser Regelung:

Ebay macht die Nutzung seiner Plattform von der Einwilligung zur Verwendung personenbezogener Daten zu Werbezwecken abhängig. Das Oberlandesgericht Brandenburg urteilte, dass Ebay nicht in einer marktbeherrschenden Stellung sei (ungeachtet eines Marktanteils von über 70 Prozent für den Bereich Online-Auktionen), so dass Verbraucher einen Zugang zu einem ähnlichen Dienst in *zumutbarer Weise* haben. Da die nun vorgeschlagene Regelung auch wieder auf die Zumutbarkeit abzielt, löst sie das durch Ebay aufgeworfene Problem demnach nicht. **Daher ist sie in der Praxis ungeeignet, solche Koppelungen selbst bei einem aus Verbrauchersicht eindeutig marktbeherrschenden Unternehmen zu unterbinden.**

Desweiteren ist nicht plausibel, warum die Einhaltung eines Grundrechts von der Marktdominanz eines Unternehmens abhängig gemacht werden soll. Im Markt der **sozialen Netzwerke** gibt es beispielsweise formell keine marktbeherrschenden Netzwerke. Gleichwohl wird ein Verbraucher, dessen Freunde in einem bestimmten Netzwerk Mitglied sind, auch in genau dieses Netzwerk eintreten wollen. Da soziale Netzwerke nicht interoperabel sind (Nutzer können aus einem sozialen Netzwerk nicht mit Nutzern anderer sozialer Netzwerke in Kontakt treten), sind Verbraucher gezwungen, in ein bestimmtes Netzwerk einzutreten, wenn sie es zusammen mit Freunden nutzen wollen. Wird der Zugang dann auch noch von der umfänglichen Preisgabe der Daten abhängig gemacht (wie es gängige Praxis ist), besteht für Verbraucher keine Wahlfreiheit ganz unabhängig davon, ob sich das soziale Netzwerk

in einer marktbeherrschenden Stellung befindet oder nicht. – Dieser Zwang ist gerade bei Kindern und Jugendlichen als problematisch einzustufen.

Da das vorgesehene eingeschränkte Koppelungsverbot die Problematik, die der Fall Ebay aufwirft und die Probleme mit sozialen Netzwerken nicht löst, halten wir ein **generelles Koppelungsverbot für dringend erforderlich**. - Diese Forderung wird auch vom Bundesrat in seiner Stellungnahme zum Gesetzentwurf getragen.^x Jede Art der Koppelung läuft dem Grundsatz einer freiwilligen Einwilligung zuwider. Verbraucher müssen jedoch Entscheidungen immer frei von datenschutzfremden Zwecken treffen können. Die Einhaltung des Datenschutzes als Grundrecht von Bürgern darf nicht von der Marktdominanz eines Unternehmens abhängig gemacht werden.

Zu Artikel 2 Nr. 8 (§ 42a BDSG-E)

Damit sich Verbraucher bei Datenschutzverstößen und -pannen vor einem Missbrauch ihrer Daten schützen können, ist es erforderlich, eine Informationspflicht bei Datenschutzverstößen und -pannen einzuführen. Gerade auch die Skandale bei der Deutschen Telekom AG, bei denen Kundendaten von 17 Millionen Kunden kopiert und in die Hände Unbefugter gelangt sind, oder Gefahren wie aus dem unverschlüsselten Versand von Kreditkartendaten durch die Landesbank Berlin zeigen den Handlungsbedarf auf. Die in **Nr. 8 vorgesehenen Maßnahmen zur Einführung von Informationspflichten bei Datenschutzverstößen und -pannen sind daher vom Grundsatz her sehr zu begrüßen**.

Allerdings gibt es in der Umsetzung drei Schwachstellen. Erstens ist es nicht ersichtlich, warum die Informationspflichten lediglich für privatwirtschaftliche und nicht auch für öffentliche Stellen eingeführt werden. In Anbetracht der Tatsache, dass gerade öffentliche Stellen eine Vielzahl von sensiblen Daten über Verbraucher verarbeiten und nicht davon ausgegangen werden kann, dass es bei diesen Stellen keine Datenschutzverstöße und -pannen gibt, **sollten die Informationspflichten auch für öffentliche Stellen gelten**.

Zweitens wird die Informationspflicht auf die Fälle beschränkt, in denen besonders sensible personenbezogene Daten Dritten unrechtmäßig zur Kenntnis gelangen und *schwerwiegende Beeinträchtigungen* für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen. **Wir halten die Beschränkung auf schwerwiegende Beeinträchtigungen für unverhältnismäßig**. Zum einen ist unklar, was eine schwerwiegende Beeinträchtigung darstellt. Es besteht somit Rechtsunsicherheit. So ist beispielsweise unklar, ob sich eine Bank bei massenhaftem Verlust von Kontodaten auf den Standpunkt stellen könnte, dass eine schwerwiegende Gefahr nicht bestanden habe, da unberechtigte Abbuchungen im Lastschriftverfahren widerrufen werden können. Ein solches Ergebnis wäre verbraucherfeindlich. Denn die Informationspflicht soll gerade dazu dienen, dass Verbraucher sensibilisiert werden, um Vorsichtsmaßnahmen zur Verhinderung von Missbrauch zu ergreifen. Zum anderen ist nicht nachzuvollziehen, warum Verbraucher nicht in jedem Fall darüber in Kenntnis gesetzt werden sollen, wenn ihre Daten Dritten unrechtmäßig zur Kenntnis gelangen. Dies ist umso wichtiger, da Daten flüchtig sind. Werden sie elektronisch weitergegeben, sind sie schwer zurück zu holen. Ein Schaden kann daher auch erst in der Zukunft eintreten. **Die Informationspflicht sollte daher nicht auf schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen beschränkt werden**. - Diese Forderung wird auch vom Bundesrat unterstützt.^{xi}

Drittens sieht die Regelung vor, dass die Betroffenen insbesondere in den Fällen, in denen eine Vielzahl von Personen betroffen ist, auch durch Anzeigen über den Datenschutzverstoß informiert werden können. **Wir halten diese Ausnahmeregelung für unangemessen.** Eine Information über Anzeigen stellt nicht sicher, dass alle Betroffenen auch tatsächlich Kenntnis über den Verstoß erlangen. So könnte es sein, dass nicht alle Kunden einer Bank von einer Datenschutzpanne betroffen sind. Eine allgemein gehaltene Anzeige einer Bank könnte jedoch nicht benennen, welche der Kunden betroffen sind. Potentiell Betroffene stünden demnach in der Holschuld, sich bei der Bank zu informieren. Ein solches Vorgehen stellt das Verursacherprinzip auf den Kopf. Auch stellt eine Anzeige nicht sicher, dass auch tatsächlich alle Verbraucher diese zur Kenntnis nehmen. So könnten Verbraucher verreist sein oder aber – wie im europäischen Binnenmarkt zunehmend der Fall – im Ausland leben. **Daher sollte die Ausnahmeregelung ersatzlos gestrichen werden. Von Datenschutzverstößen betroffene Verbraucher sollten in jedem Fall direkt informiert werden.**

Zu Artikel 2 Nr. 9 (§ 43 BDSG)

Die Änderungen in § 43 zielen zum einen darauf ab, die Bußgeldtatbestände zu erweitern. Zum anderen wird der Bußgeldrahmen erhöht und die Möglichkeit gegeben, den Bußgeldrahmen an den wirtschaftlichen Vorteil des Täters anzupassen.

Die **Ausweitung** der Bußgeldtatbestände ist generell zu **begrüßen**. Allerdings sollten die **Bußgeldtatbestände** auch noch auf **weitere Bereiche ausgeweitet** werden. Dies gilt insbesondere für Verstöße gegen fehlende Unterrichts- und Hinweispflichten, die Nichterteilung einer Auskunft gegenüber dem Betroffenen (sollten diese nicht im Zuge der Novellierung des BDSG im Hinblick auf Auskunftfeien und Scoring eingeführt werden), gegen Lösungs- und Berechtigungspflichten, gegen das Koppelungsverbot und bei mangelhaften technisch-organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit. - Diese Forderungen werden auch von den Bundesländern erhoben.^{xii}

Die Regelung wonach die Geldbuße den wirtschaftlichen Vorteil des Täters im Sinne von c) bb) übersteigen soll, ist **ausdrücklich zu befürworten**. Diese Regelung entspricht der Vorschrift des § 17 Abs. 4 OWiG. Allerdings sollte **präzisiert werden**, dass die Geldbuße den wirtschaftlichen Vorteil des Täters **deutlich** übersteigen soll.

Zu Artikel 2 Nr. 10 (§ 47 BDSG-E)

Der Gesetzentwurf sieht eine Übergangsregelung von drei Jahren für Datenaltbestände vor. **Die Dauer der Übergangsregelung ist nicht nachvollziehbar und deutlich zu lang.** Die Datenschutzskandale der vergangenen Monate haben gezeigt, dass der Handlungsbedarf heute besteht. Damit sich die Datenschutzpraxis für die Verbraucher möglichst umgehend verbessert, halten wir eine **Übergangsfrist von einem Jahr** für angemessen. Eine Frist von drei Jahren ist auch vor dem Hintergrund unverhältnismäßig, da Datenbestände - nach eigenen Aussagen von Unternehmen - bereits innerhalb von ein bis anderthalb Jahren veraltet sind. - Diese Forderung wird auch vom Bundesrat geteilt.^{xiii}

Zu Artikel 3 Nr. 3 (§ 12 TMG)

Analog zur Einführung von Informationspflichten bei Datenschutzverstößen und -pannen in § 42a BDSG-E wird nun auch eine Informationspflicht im Telemediengesetz eingeführt. Zwar ist dieser Schritt zu begrüßen, allerdings werden Unzulänglichkeiten aus dem § 42a BDSG-E auch in das TMG übernommen. Dies kommt insbesondere bei der Einschränkung zum Tragen, wonach die Regelung nur für die nicht-öffentlichen Stellen gilt und Unternehmen die Betroffenen nur bei drohenden *schwerwiegenden Beeinträchtigungen* für die Rechte oder schutzwürdigen Interessen der betroffenen Nutzer zu informieren haben (Kritik hieran siehe oben im Kommentar zu Artikel 2 Nr. 8). **Daher sollten auch öffentliche Stellen der Informationspflicht nachkommen und die Einschränkung auf schwerwiegende Beeinträchtigungen sollte gestrichen werden.**

Zu Artikel 3 Nr. 4 (§ 16 Absatz 2 TMG)

Die Nummer 4 sieht eine Streichung der Bußgeldbewährung des Koppelungsverbots vor. Zwar ist diese Streichung in dem Sinne konsequent, als dass das Koppelungsverbot gänzlich aus dem Telemediengesetz gestrichen wird. Es ist jedoch nicht plausibel, warum die Einführung des Koppelungsverbots im Bundesdatenschutzgesetz nicht auch durch eine Einführung eines Bußgeldtatbestands für den Verstoß gegen das Koppelungsverbot ergänzt wird. **Daher sollte die Ausweitung der Bußgeldtatbestände im Bundesdatenschutzgesetz auch Verstöße gegen das Koppelungsverbot umfassen.** (Siehe hierzu auch Kommentar zu Artikel 2 Nr. 9.)

Zu Artikel 4 Nr. 1 (§ 93 TKG)

Analog zur Einführung von Informationspflichten bei Datenschutzverstößen und -pannen in § 42a BDSG-E wird nun auch eine Informationspflicht im Telekommunikationsgesetz eingeführt. Zwar ist dieser Schritt zu begrüßen, allerdings werden Unzulänglichkeiten aus dem § 42a BDSG-E auch in das TKG übernommen. Dies kommt insbesondere bei der Einschränkung zum Tragen, wonach die Regelung nur für die nicht-öffentlichen Stellen gilt und Unternehmen die Betroffenen nur bei drohenden *schwerwiegenden Beeinträchtigungen* für die Rechte oder schutzwürdigen Interessen der betroffenen Nutzer zu informieren haben (Kritik hieran siehe oben im Kommentar zu Artikel 2 Nr. 8). **Daher sollten auch öffentliche Stellen der Informationspflicht nachkommen und die Einschränkung auf schwerwiegende Beeinträchtigungen sollte gestrichen werden.**

Zu Artikel 4 Nr. 2 (§ 95 Abs. 5 TKG)

Der Entwurf sieht eine Anpassung des Koppelungsverbots im Telekommunikationsgesetz an den Wortlaut des neuen Koppelungsverbots im Bundesdatenschutzgesetz vor. Da das Ziel der Anpassung darin besteht, beide Gesetze in Übereinstimmung zu bringen, ist unsere Kritik am neuen Koppelungsverbot im BDSG auch auf diese Anpassung übertragbar (siehe hierzu unseren Kommentar zu Artikel 2 Nr. 5 e)). **Anstatt ein eingeschränktes Koppelungsverbot einzuführen, müssen Koppelungsgeschäfte gänzlich verboten werden.** (Siehe hierzu auch Kommentar zu Artikel 2 Nr. 9.)

Zusätzlicher Handlungsbedarf

Der Gesetzentwurf **deckt nicht alle Regelungslücken ab**. Dies gilt insbesondere für **sechs Handlungsbereiche**.

Erstens sollte ein **Sammelrückruf für Einwilligungen** eingeführt werden. In der Regel werden von einem Anbieter auch Einwilligungen für die Weitergabe von Daten an Dritte eingeholt. Widerruft der Verbraucher seine Einwilligungen bei diesem Anbieter, ist der Widerruf jedoch nur für den jeweiligen Anbieter maßgeblich. Der Anbieter ist nach derzeitiger Rechtslage – und hieran ändert der Gesetzentwurf nichts – nicht dazu verpflichtet, den Widerruf weiter zu geben. Dieses Verfahren ist verbraucherunfreundlich. Die meisten Verbraucher werden sich nicht an das Kleingedruckte erinnern, in dem niedergelegt wurde, an welche Dritte die Daten weitergegeben wurden. Daher muss das Unternehmen, das die Einwilligung erhalten und die Daten an Dritte weiter geleitet hat, auch zur Weiterleitung des Widerrufs verpflichtet werden.

Zweitens haben die jüngsten Skandale gezeigt, dass die **Datensicherheit sowohl bei der eigenen Datenverarbeitung als auch bei der Auftragsdatenverarbeitung erhöht werden muss**. Die Tatsache, dass Mitarbeiter von Call-Centern Datenbanken kopieren konnten, zeigt, dass die derzeitigen Schutzmechanismen unzureichend sind. Auch ist es skandalös, dass die Landesbank Berlin sensible Daten unverschlüsselt an Auftragsdatenverarbeiter übermittelt. Anbieter müssen dafür sorgen, dass ein möglicher Missbrauch von Daten schon durch die technische und organisatorische Ausgestaltung verhindert wird. **Daher müssen die Anforderungen an technische und organisatorische Maßnahmen zur Verbesserung der Datensicherheit erhöht und Regelungen zur Auftragsverarbeitung verbessert werden**. (Siehe hierzu auch Anmerkungen zu Artikel 2 Nr. 1a neu und §9 und Anlage zu § 9 BDSG)

Drittens sollte eine **Kennzeichnungs- und Protokollierungspflicht** für die Herkunft und Verwendung personenbezogener Daten eingeführt werden. Durch die **Kennzeichnung** sollen Verbraucher direkt in der Werbemitteilung erfahren können, von wem die Daten stammen. Diese Information würde die Transparenz über die Datenverarbeitung erhöhen und es Verbrauchern erleichtern, ihre Daten zu sperren. Die **Protokollierung** ist eine Voraussetzung dafür, dass die betrieblichen Datenschutzbeauftragten und die Datenschutzaufsichtsbehörden die Datenverarbeitungssysteme kontrollieren und Fälle des Missbrauchs aufklären können. Wie die aktuellen Datenskandale mit Kontodaten, die der Verbraucherzentrale Bundesverband und die *Wirtschaftswoche* aufgedeckt haben, zeigen, führt das Fehlen einer Protokollierung zudem dazu, dass Verbraucher nicht wissen, was mit ihren Daten gemacht wurde, an wen die Daten unzulässiger Weise übermittelt wurden und ihnen wird die Möglichkeit genommen, die Löschung ihrer Daten durchzusetzen. **Nur durch eine Protokollierung kann sichergestellt werden, dass Schaden von Verbrauchern abgewendet wird und sie für die Löschung ihrer Daten sorgen können**. - Diese Forderung wird auch vom Bundesrat erhoben.^{xiv}

Viertens müssen **Verbraucherverbände mit dem Recht ausgestattet werden, gegen Datenschutzverstöße zu klagen**. Verbraucherorganisationen sind im Bereich des Datenschutzes häufig die Hände gebunden, da das Datenschutzrecht von den Gerichten nicht als verbraucherschützende Norm im Sinne des § 2 des Unterlassungsklagegesetzes (UKlaG) anerkannt wird. Kommt ein Unternehmen beispielsweise den gesetzlichen Verpflichtungen nicht nach, Verbraucher über die gespeicherten Daten Auskunft zu erteilen oder vewendet das Unternehmen die Daten

zu Zwecken, für die keine Einwilligung vorliegt, können Verbraucherorganisationen ihre Verbandsklagebefugnisse nicht einsetzen. – Gesetzeswidriges Verhalten bleibt demnach häufig unsanktioniert, da der einzelne Verbraucher den Aufwand scheut zu klagen. Analog beispielsweise zu den Klagerechten im Bereich des unlauteren Wettbewerbs (UWG) sollten Verbraucher durch qualifizierte Verbraucherorganisationen auch im Datenschutz präventiv geschützt werden. **Daher bedarf es einer Klarstellung im UKlaG, nach der Datenschutzvorschriften, soweit sie die Rechte der Verbraucher betreffen, Verbraucherschutzgesetze im Sinne des UKlaG darstellen.** Diese Forderung wird auch von den Bundesländern unterstützt.^{xv}

Fünftens müssen die **Datenschutzaufsichtsbehörden personell besser ausgestattet werden.** In einigen Bundesländern ist ein einziger Mitarbeiter in den Aufsichtsbehörden für die Überwachung von über einhunderttausend Unternehmen zuständig. Es ist daher nicht verwunderlich, dass die Behörden oft erst dann reagieren, wenn die Datenschutzskandale publik werden – das Kind also schon in den Brunnen gefallen ist. **Daher müssen die Bundesländer dafür Sorge tragen, dass die staatliche Überwachung auf einem soliden personellen Fundament steht.**

Sechstens sollte den Aufsichtsbehörden in § 38 Abs. 5 BDSG auch die Befugnis gegeben werden, erhebliche materiell-rechtliche Datenschutzverstöße zu untersagen. Nach derzeitiger Rechtslage bleibt den Aufsichtsbehörden nur die Möglichkeit, sehenden Auges einen Datenschutzverstoß abzuwarten, um ihn anschließend zu ahnden. Dieses Verfahren ist inkonsequent, da nach Gesetzeslage eine Untersagung im Fall von *Datensicherheitsmängeln* möglich ist. Verbraucher können jedoch nicht nur durch Sicherheitsmängel geschädigt werden, sondern – und viel bedeutender – auch wenn die Daten unzulässig verarbeitet werden. **Daher muss auch für den Fall einer offensichtlich unzulässigen Datenverarbeitung die Möglichkeit einer Untersagung bestehen.**

2. Bewertung des Entwurfs eines Gesetzes zur Regelung des Datenschutzaudits (Artikel 1)

Ein Datenschutzsiegel auf der Grundlage eines Audits kann Verbrauchern auf den ersten Blick vermitteln, dass ein Produkt, eine Dienstleistung oder ein Verfahren den produkt- bzw. anwendungsspezifischen Datenschutz- und Datensicherheitsanforderungen genügt. Entscheidend für die Aussagekraft eines Siegels ist, dass es drei wesentliche Kriterien erfüllt. Es muss **glaubwürdig** sein. Das heißt, dass es von kompetenten und unabhängigen Instanzen in einem transparenten Verfahren vergeben werden muss. Es muss **aussagekräftig** sein. Aussagekräftig ist ein Siegel dann, wenn die Datenschutzkonformität am Produkt, der Dienstleistung oder dem Verfahren selbst sichtbar wird. Ferner muss ein Datenschutzsiegel **vergleichbar** sein. Das bedeutet, dass sich die Überprüfung der Datenschutzkonformität von gleichen Produkten, Dienstleistungen und Verfahren unterschiedlicher Anbieter an einheitlichen Kriterien orientieren muss. Hier darf es keine Unterschiede zwischen Kontrollstellen und Bundesländern geben.

Diese Anforderungen werden durch den Entwurf eines Datenschutzauditgesetzes vom 10. Dezember 2008 nur zum Teil erfüllt. **Positiv** am Entwurf ist insbesondere, dass:

- § die Vergabe eines Siegels nur dann erfolgen soll, wenn **über die Einhaltung der Gesetze hinaus** Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit **erfüllt werden** (§ 1 DSAG-E);
- § **Kontrollstellen** nur tätig werden können, sofern ihr Leitungspersonal und die für die Kontrollen verantwortlichen Beschäftigten die persönliche **Zuverlässigkeit, Unabhängigkeit und fachliche Eignung** für das Datenschutzaudit **nachweist** (§§ 4 und 5 DSAG-E) und
- § ein **Datenschutzauditausschuss** damit beauftragt wird, Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit zu erlassen (§ 11 DSAG-E).

Zu **kritisieren** ist jedoch, dass:

- § aus dem Gesetzestext nicht klar hervor geht, dass der **Gegenstand von Auditierungen** auch **Produkte, Dienstleistungen und Verfahren umfasst**;
- § **Aufsichtsbehörden nicht auch das Recht erhalten, die Güte von Gutachten der Kontrollstellen zu überprüfen**, um ggf. die Zulassung zu entziehen (§§ 4 und 7 DSAG-E);
- § das **Verzeichnis über die Auditierungen** beim BfDI **nicht auch die Gutachten enthalten** soll (§ 8 DSAG-E) und
- § **keine Verbrauchervertreter im Datenschutzauditausschuss vorgesehen** sind, Unternehmensvertreter hingegen schon (§ 12 DSAG-E).

In unserer Stellungnahme vom 15. Oktober 2007 zum *Entwurf eines Bundesdatenschutzauditgesetzes vom 7. September 2007* haben wir uns für ein zweistufiges Auditierungsverfahren ausgesprochen. In einem solchen Verfahren erstellen die Kontrollstellen ein Gutachten, das von einer auf Bundesebene zu schaffenden Zentralstelle geprüft wird. Die Zentralstelle vergibt dann das Siegel und nimmt einen Eintrag in ein Register vor. Wir haben ein solches zweistufiges Verfahren aus zwei Gründen befürwortet. Erstens erhöht die Überprüfung der Gutachten durch einen unabhängigen Dritten die Glaubwürdigkeit des Audits. Es steht zu befürchten, dass in einem einstufigen Verfahren die Kontrollstellen bevorzugt werden, die möglichst unkritische Begutachtungen bzw. Gefälligkeitsgutachten durchführen. Zweitens zeigt die Erfahrung mit Datenschutzauditierungen, dass die Güte von Gutachtern gerade auch wegen der Auslegungsbedürftigkeit der Datenschutzgesetzgebung stark variiert. Eine Plausibilitätskontrolle durch einen Dritten würden die Konsistenz der Güte erhöhen. Zwar sieht der Referentenentwurf kein zweistufiges Verfahren vor, allerdings wurden eine Reihe von Qualitätssicherungsmaßnahmen installiert, die unsere Bedenken gegenüber einem einstufigen Verfahren mildern. **Es ist jedoch sicherzustellen, dass die Aufsichtsbehörden die Zulassung auch in den Fällen entziehen können, in denen die Gutachten unplausibel sind.**

Zu § 1 (Datenschutzaudit)

Der Verbraucherzentrale Bundesverband **begrüßt es ausdrücklich**, dass die Vergabe eines Siegels nur dann erfolgen soll, wenn **über die Einhaltung der Gesetze hinaus**

Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit erfüllt werden.

Allerdings sollte der Gesetzestext eindeutiger zum Ausdruck bringen, dass der Auditgegenstand auch Produkte und Dienstleistungen umfasst. Dass dies die Intention der Verfasser ist, geht aus der Gesetzesbegründung, nicht jedoch aus den im Gesetzestext verwendeten Begriffen „Datenschutzkonzept“ und „informationstechnische Einrichtung“ hervor. Aus Verbrauchersicht ist gerade der Fokus am konkreten Produkt bzw. der konkreten Dienstleistung (wie Rabattprogramm, soziales Netzwerk oder Kontaktbörse) entscheidend. – Kaufen Verbraucher eine Software, wollen sie sicher gehen, dass die Software sie nicht heimlich ausspioniert und dass die Software sicher ist. Besuchen Verbraucher Kontaktbörsen im Internet, wollen sie sicher gehen, dass ihre Daten nicht missbraucht werden. **Diese Intention sollte auch im Gesetzestext deutlich werden.**

Zu §§ 4 und 7 (Zulassung der Kontrollstelle und Entziehung der Zulassung und Pflichten der zuständigen Behörde)

Der Entwurf sieht vor, dass die Zulassung einer Kontrollstelle in Fällen entzogen werden kann, wenn sie u.a. den Anforderungen des § 4 Abs. 1 DSAG-E nicht genügt.

Diese Regelung ist unzureichend. Auch die fachlich best ausgestattete Kontrollstelle kann Gefälligkeitsgutachten erstellen. **Daher müssen die Aufsichtsbehörden auch das Recht erhalten, die Güte der Gutachten der Kontrollstellen zu überprüfen und bei Verdacht auf Gefälligkeitsgutachten die Zulassung entziehen können.**

Zu § 9 (Datenschutzauditsiegel, Verzeichnisse)

Im § 9 Abs. 1 DSAG-E wird geregelt, dass der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ein Verzeichnis über die Auditierungen zu führen hat. Unverständlicherweise soll dieses Verzeichnis jedoch nicht auch die Gutachten bzw. Zusammenfassungen der Gutachten enthalten. Die Aufnahme der Gutachten ist jedoch gerade für die Transparenz wesentlich. Nur wenn die Öffentlichkeit und die Wissenschaft die Gutachten einsehen können, können Unzulänglichkeiten aufgedeckt werden. **Daher muss in die Aufzählung des § 9 Abs. 1 DSAG-E auch noch das Gutachten oder zumindest eine Zusammenfassung des Gutachtens aufgenommen werden.**

Zu § 11 (Datenschutzauditausschuss)

Der Verbraucherzentrale Bundesverband begrüßt es sehr, dass ein Ausschuss beauftragt werden soll, Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit zu erlassen.

Allerdings ist zu fragen, ob ein neues Gremium geschaffen werden muss, oder ob es nicht **sinnvoller wäre, auf bestehende Institutionen zurück zu greifen.** In Frage kämen der Düsseldorfer Kreis oder die Konferenz der Datenschutzbeauftragten des Bundes und der Länder. Eine solche Lösung würde den Aufbau von Parallelstrukturen vermeiden und könnte Bürokratie reduzieren. Gleichzeitig ist die fachliche Kompetenz sichergestellt.

Zudem sollte in die Auflistung des Absatzes 1 noch **ein Punkt zur Verbesserung der Datensicherheit** aufgenommen werden:

5. technische und organisatorische Maßnahmen zur Datensicherheit.

Die jüngsten Datenschutzskandale haben gezeigt, dass gerade im Bereich der Datensicherheit ein großer Handlungsbedarf besteht.

Zu § 12 (Mitglieder des Datenschutzauditausschusses)

Nicht nachvollziehen kann der Verbraucherzentrale Bundesverband, dass unter den Mitgliedern des Datenschutzauditausschusses keine Vertreter von Verbraucherorganisationen vorgesehen sind. Durch wegweisende Verfahren, Studien und durch die Verbraucherberatung Vorort haben die Verbraucherorganisationen in den vergangenen Jahrzehnten entscheidende Beiträge für die Fortentwicklung des Datenschutzes geleistet. Gerade vor dem Hintergrund der Kommerzialisierung von Verbraucherdaten ist es **erforderlich, dass zumindest zwei Vertreter von unabhängigen Verbraucherorganisationen als Mitglieder des Datenschutzauditausschusses vorgesehen sind**. Datenschutz ist heute auch Verbraucherschutz. – Ähnliches gilt auch für Arbeitnehmervertreter.

i

http://www.vzbv.de/start/index.php?page=themen&bereichs_id=1&themen_id=4&dok_id=771&search_1=datenschutz&search_2=&highlighting=yes

ii http://www.vzbv.de/mediapics/einwilligungserklaerungen_datenschutz_02_09_2008.pdf

iii

http://www.bmi.bund.de/Internet/Content/Common/Anlagen/Gesetze/Entwurf__BDSG,templateId=raw,property=publicationFile.pdf/Entwurf_BDSG.pdf

iv Stellungnahme des Bundesrates vom 13.02.09, Drucksache 4/09 (Beschluss), Nummer 4.

v <http://de.statista.org/statistik/daten/studie/1758/umfrage/aussagen-zum-thema-datenschutz-in-deutschland/>

vi <http://de.statista.org/statistik/daten/studie/1758/umfrage/aussagen-zum-thema-datenschutz-in-deutschland/>

vii <http://www.freiheit-der-kommunikation.de/>

viii „Novellierung des Bundesdatenschutzgesetzes trifft Verbraucher und Wirtschaft“, Gemeinsame Broschüre der Deutschen Post AG, arvato AG, Schober Information Services GmbH, DDV Deutscher Dialogmarketing Verband e.V. und bvH Bundesverband des Deutschen Versandhandels, S. 12.

ix Direkt marketing, Februar 2009, S. 13-15.

x Stellungnahme des Bundesrates vom 13.02.09, Drucksache 4/09 (Beschluss), Nummer 15.

xi Stellungnahme des Bundesrates vom 13.02.09, Drucksache 4/09 (Beschluss), Nummer 19.

xii Stellungnahme des Bundesrates vom 13.02.09, Drucksache 4/09 (Beschluss), Nummer 23, 24 und 25.

xiii Stellungnahme des Bundesrates vom 13.02.09, Drucksache 4/09 (Beschluss), Nummer 28.

xiv Stellungnahme des Bundesrates vom 13.02.09, Drucksache 4/09 (Beschluss), Nummer 34 b).

xv Stellungnahme des Bundesrates vom 13.02.09, Drucksache 4/09 (Beschluss). Nummer 34 a).