verbraucherzentrale Bundesverband

30. Oktober 2008

Verbrauchersouveränität im Datenschutz herstellen

Stellungnahme
des Verbraucherzentrale Bundesverbandes

zum Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes und zur Regelung des Datenschutzaudits vom 22. Oktober 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 Wochen und Monate haben eindringlich vor Augen geführt, dass das **Bundesdatenschutzgesetz** Verbraucher **unzureichend vor einem Missbrauch ihrer Daten schützt**. Binnen 44 Stunden und für 850 Euro konnte der Verbraucherzentrale Bundesverband 6 Millionen Datensätze erwerben, bei denen 4 Millionen Datensätze Kontoverbindungsdaten enthielten.[1] Die Deutsche Telekom AG musste in diesem Jahr 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 vor zwei Jahren in die Hände Unbefugter gelangten.

Diese Beispiele verdeutlichen den Handlungsbedarf im Datenschutz. **Ziel** muss es daher sein, **die Verbrauchersouveränität im Datenschutz herzustellen.**

Die **Schutzlücken** bestehen insbesondere in den **folgenden vier Bereichen**:

- Durch das Listenprivileg können bestimmte Daten über Verbraucher auch **ohne** deren **Einwilligung** für Werbe- und Marketingzwecke übermittelt und genutzt werden – der Verbraucher kann somit keine Kontroll- und Steuerungsfunktion über die Verwendung seiner Daten ausüben.
- Werden von Verbrauchern Einwilligungen in die Datenverarbeitung zu Werbe- und Marketingzwecken eingeholt, können diese von Verbrauchern häufig nicht bewusst erteilt werden, da die **Einwilligungen schwer- oder missverständlich formuliert sind** oder aber der Zugang zu einem gewerblichen Angebot wird davon abhängig gemacht, dass Verbraucher in die Datenübermittlung einwilligen (**Koppelungsgeschäft**).
- Die Daten sind unzureichend vor dem unbefugten Kopieren, der unbefugten Weitergabe und Verarbeitung geschützt (**mangelnde Datensicherheit**).
- **Sanktionen** gegen Datenschutzvorschriften sind **zu lasch** und **Anreize** für einen verbraucherfreundlichen Umgang mit personenbezogenen Daten sind **unzureichend**.

Die Bundesregierung hat auf die Datenschutzskandale der Sommermonate mit dem Entwurf eines *Gesetzes zur Änderung des Bundesdatenschutzgesetzes und zur Regelung des Datenschutzaudits* vom 22. Oktober 2008 prompt reagiert. Der Entwurf stellt durch die **Abschaffung des Listenprivilegs** und die **Einführung von Anforderungen** an Einwilligungen einen **notwendigen Schritt in die richtige Richtung** dar. Der Entwurf beendet die bestehende Rechtslage, wonach der *Widerruf* 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.

In entscheidenden Punkten geht der Entwurf jedoch nicht weit genug:

Erstens widersprechen einige der neuen Regelungen in § 28 Abs. 3 Nr. 1 BDSG-E Vorschriften in der europäischen Datenschutzrichtlinie und im UWG – hier gilt es daher, die Regelungen an bestehende Vorschrift anzugleichen.

Zweitens ist in § 28 Abs. 3b BDSG-E ein **generelles Koppelungsverbot** einzuführen. Das vorgeschlagene eingeschränkte Koppelungsverbot ist unzureichend.

Drittens sind die **Bußgeldtatbestände** in § 43 BDSG noch weiter als vorgeschlagen **auszuweiten**.

Viertens 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 einer Protokollierungspflicht,** die **Stärkung des kollektiven Rechtsschutzes** und **die Stärkung der Eingriffsbefugnisse für die Aufsichtsbehörden**.

Fünftens 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 es sich nicht auch auf Produkte, Dienstleistungen und Verfahren erstreckt** und dass in **dem neuen Datenschutzauditausschuss keine Verbrauchervertreter vorgesehen** sind.

Durch die kurze Frist zur Stellungnahme beschränkt sich die folgende Bewertung des Gesetzentwurfs auf wesentliche Punkte und ist daher nicht vollständig. Zudem behalten wir uns vor, weitere Anmerkungen auch noch nach Fristablauf einzureichen.

1. Bewertung des Entwurfs eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes

Zu Artikel 1 Nr. 5 (§ 28)

Zu a) und b)

Das Hauptziel der Änderungen in a) und b) besteht in der Streichung des bisher in § 28 Abs. 3 Satz 1 Nr. 3 BDSG geregelten Listenprivilegs. Die Abschaffung des Listenprivilegs ist entscheidend, um Verbrauchern die Kontrolle über die Verwendung ihrer Daten zurück zu geben. Daher **begrüßen wir die Neufassungen der Absätze 2 und 3 grundsätzlich.**

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

Erstens wird die Verarbeitung oder Nutzung für Zwecke der Werbung nicht beschränkt 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**.

Zweitens 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.

Drittens darf die neue Regelung nicht als Freibrief für jedwede Werbeform gelten. Die vorgeschlagene Vorschrift ist so offen formuliert, dass diese ohne Weiteres auch die Telefonwerbung legitimiert, die per se nur unter den engen Voraussetzungen des § 7 Abs. 2 Nr. 2 UWG zulässig ist (Einwilligung). Nur weil ein Kunde beispielsweise bei einer Bestellung über das Internet neben seiner Postadresse auch seine Telefonnummer angegeben hat, darf die Preisgabe der Telefonnummer nicht gleichgesetzt werden, mit der Einwilligung in die Telefonwerbung. Eine solche Regelung würde der aktuell diskutierten Novellierung des UWG zuwider laufen, wonach die Telefonwerbung nur nach **ausdrücklicher** Einwilligung erfolgen darf. Daher muss in der Nummer 1 des Absatzes 3 **klar gestellt** werden, dass die Daten nur für die **Briefwerbung und die elektronische Werbung verwendet werden dürfen.**

Zu c)

Hauptziele der Änderungen in c) 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'.

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 3 a BDSG-E ergänzt werden: bezüglich der Hinweispflichten gilt § 4 a Abs. 1 Satz 2 BDSG entsprechend. Zudem sollte im Satz 3 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**. Am Beispiel Ebay wird die Schwäche der neuen Regelung deutlich. 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), sodass Verbraucher einen Zugang zu einem

ähnlichen Dienst in zumutbarer Weise haben. Da die vorgeschlagene Regelung auch wieder auf die Zumutbarkeit abzielt, löst sie das durch Ebay aufgeworfene Problem nicht. Daher halten wir ein **generelles Koppelungsverbot für dringend erforderlich**. Jede Art der Koppelung läuft dem Grundsatz einer freiwilligen Einwilligung zuwider. Verbraucher müssen jedoch Entscheidungen frei von datenschutzfremden Zwecken treffen können.

Zu Artikel 1 Nr. 8 (§ 43)

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

Die **Ausweitung** des Bußgeldtatbestandes von der unbefugten Erhebung oder Verarbeitung personenbezogener Daten auch auf die unbefugte Nutzung dieser Daten, ist zu **begrüßen** (§ 43 Abs. 2 Nr. 1). Allerdings sollten die **Bußgeldtatbestände** auch noch auf **weitere Bereiche ausgeweitet** werden. Dies gilt insbesondere für Verstöße gegen fehlende Unterrichtung, die Nichterteilung einer Auskunft gegenüber dem Betroffenen (sollten diese nicht im Zuge der Novellierung des BDSG im Hinblick auf Auskunfteien und Scoring eingeführt werden) und gegen Löschungs- und Berechtigungspflichten.

Die Regelung wonach die Geldbuße den wirtschaftlichen Vorteil des Täters im Sinne von b) 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 1 Nr. 9 (§ 44a)

Damit sich Verbraucher bei Datenschutzpannen vor einem Missbrauch ihrer Daten schützen können, ist es erforderlich, eine Informationspflicht bei Datenschutzpannen einzuführen. Gerade auch der jüngst bekannt gewordene Skandal bei der Deutschen Telekom AG, wonach Kundendaten von 17 Millionnen Kunden kopiert und in die Hände Unbefugter gelangt sind, zeigt den Handlungsbedarf auf. Die in **Nr. 9 vorgesehenen Maßnahmen sind daher sehr zu begrüßen**.

Zu Artikel Nr. 10 (§ 47)

Der Gesetzentwurf sieht eine Übergangsregelung für Datenaltbestände vor, lässt jedoch offen, wie lange diese Übergangsregelung Bestand hat. Damit sich die Datenschutzpraxis für die Verbraucher möglichst umgehend verbessert, halten wir eine **Übergangsfrist von einem Jahr** für angemessen.

Zusätzlicher Handlungsbedarf

Der Gesetzentwurf **deckt nicht alle Regelungslücken ab.** Dies gilt insbsondere für **fünf 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 sein.

Zweitens haben die jüngsten Skandale gezeigt, dass die **Datensicherheit sowohl bei der eigenen Datenverabreitung 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. Die Anbieter müssen dafür sorgen, dass ein möglicher Missbrauch von Daten schon durch die technische und organisatorische Ausgestaltung verhindert wird. Technische und organisatorische Maßnahmen müssen ergriffen werden, um einen spürbaren Beitrag zur Verbesserung der Datensicherheit zu leisten.

Drittens sollte eine **Protokollierungspflicht** für die Herkunft und Verwendung personenbezogener Daten eingeführt werden. Die Protokollierung ist eine Voraussetzung dafür, dass die betrieblichen Datenschutzbeauftragten und die Datenschutzaufsichtsbehörden die Datenverarbeitungssysteme kontrollieren und Fälle des Missbrauchs aufklären können. Wie der aktuelle Datenskandal mit den Kontodaten zeigt, 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.

Viertens ist es erforderlich den **kollektiven Rechtsschutz im Bereich des Datenschutzes zu stärken**. Die Gerichte erkennen regelmäßig nicht an, dass es sich bei Datenschutzgesetzen um Verbraucherschutzgesetze im Sinne des Unterlassungsklagegesetzes (UKlaG) handelt. Daher bedarf es eines Hinweises entweder im BDSG sowie im Telemediengesetz oder im UKlaG, dass Datenschutzvorschriften, soweit sie die Rechte der Verbraucher betreffen, Verbraucherschutzgesetze im Sinne des UKlaG sind.

Fünftens 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 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 der Regelung des Datenschutzaudits

In seiner Stellungnahme vom 15. Oktober 2007 zum *Entwurf eines Bundesdatenschutzauditgesetzes vom 7. September 2007* hat der Verbraucherzentrale Bundesverband seine Erwartungen an ein verbraucherfreundliches Datenschutzaudit formuliert. Demnach sollte ein Datenschutzsiegel auf der Grundlage eines Audits Verbrauchern auf den ersten Blick vermitteln, dass ein Produkt, eine Dienstleistung oder ein Verfahren den produkt- bzw. anwendungsspezifischen Datenschutz- und Datensicherheitsanforderungen genügt. Entscheident 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 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 22. Oktober 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);
- **nicht-öffentlichen Stellen** mindestens **einmal im Jahr kontrolliert werden** (§ 3 DSAG-E);
- **Kontrollstellen** nur tätig werden können, sofern ihr Leitungspersonal und die für die Kontrollen verantworlichen Beschäftigten die persönliche **Zuverlässigkeit, Unabhängigkeit und fachliche Eignung** nach § 9 BDSG für das Datenschutzaudit **nachweist** (§§ 4 und 9 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:

- der **Gegenstand von Auditierungen** auf das Datenschutzkonzept und die technische Einrichtung beschränkt ist und **nicht auch Produkte, Dienstleistungen und Verfahren umfasst;**
- das **Verzeichnis über die Auditierungen** beim BfDI **nicht auch die Gutachten enthalten** soll (§ 8 DSAG-E) und
- **kein Verbrauchervertreter im Datenschutzauditausschuss vorgesehen** ist (§ 12 DSAG-E).

In unserer Stellungnahme vom 15. Oktober 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 Glaubwürdikeit des Audits. Glaubwürdigkeit ist wiederum entscheidend für die Akzeptanz des Siegels durch die Verbraucher. 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. **Allerdings muss der Gegenstandsbereich der Audits unbedingt auch auf Produkte, Dienstleistungen und Verfahren erweitert werden und Verbrauchervertreter müssen im Datenschutzauditausschuss vertreten sein.**

Zu § 1 (Datenschutzaudit)

Der Verbraucherzentale 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 (§ 1 Satz 2 Nr. 2 DSAG-E). **Allerdings ist die Beschränkung des Auditgegenstandes** auf das **Datenschutzkonzept und die technische Einrichtung zu eng (§1 DSAG-E)**. Verbraucher wollen wissen, ob das Produkt oder die Dienstleistung, die sie kaufen oder ein Verfahren, das sie nutzen, den Anforderungen des Datenschutzes genügen. Für sie ist es in vielen Fällen zweitrangig, ob der Anbieter ein Datenschutzkonzept hat oder ob die technische Einrichtung des Anbieters mit dem Datenschutz kompatibel ist. Daher muss die Definition des Gegenstands des Datenschutzaudits um Produkte, Dienstleistungen und Verfahren erweitert werden. – 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.

Wenn also das Datenschutzaudit für Unternehmen einen Wettbewerbsvorteil mit sich bringen soll, müssen auch **Produkte, Dienstleistungen und Verfahren Gegenstand eines Datenschutzaudits sein.** Ansonsten wird sich die Nachfrage nach entsprechend gekennzeichneten Produkten nicht einstellen. – Eine Ausweitung des Auditgegenstands hätte jedoch weitreichende Konsequenzen nicht nur für § 1 DSAG-E. Denn der Entwurf geht durchgehend lediglich von der Auditierung von Datenschutzkonzepten und technischen Einrichtungen aus. Für die Auditierung von Produkten, Dienstleistungen und Verfahren sind jedoch teilweise andere Anforderungen notwendig. So ist beispielsweise die Anforderung nach der die organisatorische Stellung des Beauftragten für den Datenschutz eingehalten werden muss (§ 1 Satz 2 Nr. 3 DSAG-E) für ein Produkt oder eine Dienstleistung irrelevant.

Zu § 8 (Datenschutzauditsiegel, Verzeichnisse)

Im § 8 Abs. 2 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 wesentilch. Nur wenn die Öffentlichkeit und Wissenschaft

die Gutachten einsehen kann, können Unzulänglichkeiten aufgedeckt werden. **Daher muss in die Aufzählung des § 8 Abs. 2 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 sicher gestellt.

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

4. 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 vor Ort haben die Verbraucherorganisationen in den vergangenen Jahrzehnten entscheidende Beiträge für die Fortentwicklung des Datenschutzes geleistet. Gerade vor dem Hintergrund der Kommerziallisierung von Daten ist es **erforderlich**, **dass zumindest zwei Vertreter von unabhängigen Verbraucherorganisationen als Mitglieder des Datenschutzauditausschusses vorgesehen sind.** Ähnliches gilt auch für Arbeitnehmervertreter.

---

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